INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

2009 情財第 834 号

MFP の脆弱性に関する調査報告書

V1.0

独立行政法人 情報処理推進機構
セキュリティセンター

2010 年 8 月

本文中の製品名は、一般に各社の登録商標、商標、または商品名である。
本文では、TM、©、®マークは省略している。

目次

目次 2
図目次 5
表目次 7
1. はじめに 8
1.1 MFPとは 8
1.2 本書の背景 8
1.3 本書の目的 8
1.4 対象とする読者 9
1.5 本書の前提と範囲 9
2. 調査分析手法 10
2.1 MFPの用途と機能を整理 11
2.2 機能ブロックの整理 11
2.3 守るべき資産として機能ブロック間で交換されるデータを特定 11
2.4 脆弱性の分類 12
2.5 各資産に対して脅威と脆弱性を列挙 12
3. MFPの用途、機能 13
3.1 MFPの発展の経緯 13
3.2 MFPに求められるセキュリティ 14
3.3 MFPを利用する環境でのライフサイクル 15
3.4 情報システムから見たMFP 17
3.5 他の組織との間から見たMFPの利用システム 19
3.6 利用者環境でのMFPの各システムの用途 20
3.7 MFPのシステム構成例 20
3.8 MFP内部のハードウェア 22
3.9 MFP内部のソフトウェア 27
4. MFP利用時のデータフロー 33
4.1 プリント 34
4.2 負荷分散印刷 35
4.3 スキャン to X、ファクス送信 36
4.4 ファクス受信 38
4.5 コピー 39
4.6 構成管理情報の設定、取得(コンソール) 40
4.7 遠隔通信経由での構成管理情報の設定、取得 41

4.8 保守作業 部品交換、課金取得、診断 42
5. MFPの守るべき資産 43
5.1 MFPを利用する環境での一次資産 43
5.2 MFPを利用するために守るべき対象としての二次資産 43
5.3 MFP本体 44
5.4 実行時データ 45
5.5 他システム 46
5.6 稼動結果情報 47
6. 脆弱性の分類 49
6.1 CWE共通の脆弱性タイプと、本資料で扱う分類 49
7. 脅威から想定される脆弱性 51
7.1 脅威の抽出 51
7.2 本体機器（ハードウェア) 53
7.3 MFP内ソフトウェア 56
7.4 使用ライセンス、保守ライセンス 60
7.5 着脱式メディア(利用者用、管理者/保守者用) 62
7.6 ジョブデータ（イメージ,宛先,制御) 65
7.7 管理構成情報 70
7.8 電子証明書、ID、パスワード、セッション情報(本体内、他システム内) 73
7.9 正しい時刻 80
7.10 原稿、印刷物 84
7.11 MFP内共有ファイル 87
7.12 利用履歴、監査記録 91
7.13 MFP利用課金情報 95
7.14 通信システム(スイッチ、DHCP, DNS, NTPを含む) 98
7.15 遠隔管理システム 102
7.16 一般利用者端末 107
7.17 蓄積・外部処理(スプーラ、共有フォルダ、メール、業務システム) 111
8. 脆弱性の詳細解説 115
9. ユニット間でデータを盗聴される問題 116
9.1 概要 116
9.2 解説 116
9.3 対策 118
9.4 参考情報 118
9.5 CVSS深刻度評価(参考値) 120
10. ドライバ用プロトコルを経由した侵入の問題 121

10.1 概要 121
10.2 解説 121
10.3 対策 124
10.4 参考情報 124
10.5 CVSS深刻度評価(参考値) 126
11. 複数配信を一括して実行する機能による問題 127
11.1 概要 127
11.2 解説 127
11.3 対策 130
11.4 参考情報 130
11.5 CVSS深刻度評価(参考値) 131
12. 多数のプロトコルに含まれる脆弱性による問題 132
12.1 概要 132
12.2 解説 132
12.3 対策 141
12.4 参考情報 141
12.5 CVSS深刻度評価(参考値) 143
13. 遠隔保守インタフェースの悪用から起こる問題 144
13.1 概要 144
13.2 解説 144
13.3 対策 148
13.4 参考情報 148
13.5 CVSS深刻度評価(参考値) 149
14. 着脱式媒体を利用したMFPの構成変更による問題 150
14.1 概要 150
14.2 解説 150
14.3 対策 152
14.4 参考情報 152
14.5 CVSS深刻度評価(参考値) 153
15. まとめ 154

図目次

図 2-1 調査分析手法の概要 10
図 3-1 MFPの発展の経緯 13
図 3-2 MFPに求められる機能、セキュリティ 14
図 3-3 MFPを利用する環境でのライフサイクル 16
図 3-4 情報システムから見たMFP 17
図 3-5 他の組織との間から見たMFPの利用システム 19
図 3-6 MFPのシステム構成例 21
図 3-7 MFP内部のハードウェア 22
図 3-8 MFP内部のハードウェア - 実行基盤と主なインタフェース 24
図 3-9 MFP内部のハードウェア - ユニットまたはモジュール間の接続 25
図 3-10 MFP内部のソフトウェア 27
図 4-1 MFP利用時のデータフローの構成図 33
図 4-2 プリントのデータフロー 34
図 4-3 負荷分散印刷のデータフロー 35
図 4-4 スキャン to X、ファクス送信のデータフロー 36
図 4-5 ファクス受信のデータフロー 38
図 4-6 コピーのデータフロー 39
図 4-7 構成管理情報の設定、取得データフロー 40
図 4-8 遠隔通信経由での構成管理情報の設定、取得データフロー 41
図 4-9 保守作業 部品交換、課金取得、診断のデータフロー 42
図 5-1 MFP利用時のデータフロー 43
図 6-1 CWE共通の脆弱性タイプと、本資料で扱う分類 49
図 7-1 情報セキュリティの要求事項 – 7 つのタイプ 51
図 9-1 スキャンユニットと実行基盤の間にUSBモニタを挿入した図 116
図 9-2 MFP内部のユニットまたはモジュールの接続構成例 118
図 10-1 ドライバ用プロトコルLPRを経由した侵入の例 121
図 10-2 ドライバ用プロトコルLPRコマンドによる侵入のシーケンス例 122
図 11-1 複数配信を一括して実行する例 127
図 12-1 MFPで一般的に利用される通信プロトコルの一覧 132
図 13-1 HTTPリクエスト強要(CSRF)を利用したMFPの保守インタフェース悪用例 144
図 13-2 MFP機器内部の保守インタフェース 145
図 13-3 その他のMFPの保守インタフェースへのアクセス方法例 146
図 13-4 CSRFを利用した保守インタフェース悪用のシーケンス例 147

図 14-1 SDメモリカードによるMFPの一括更新による問題 151

表目次

表 3-1 利用者環境でのMFPの各システムの用途 20
表 5-1 MFPを利用するために守るべき対象としての二次資産 44
表 6-1 本資料で利用する脆弱性タイプ 50
表 10-1 MFPで利用されている主なドライバプロトコル 123

1. はじめに

1.1 MFPとは

MFP とは、Multi Function Peripheral(多機能周辺機器)、Multi Function Printer(多機能プリンタ)または Multi Function Product(多機能製品）の略称である。MFD (Multi Function Device: 多機能機器)と呼ぶこともある。

本書では MFP は機能的に、コピー、プリンタ、スキャナ、ファクスの機能が一体になった機器のことを指している。

また、本書での調査対象は特に MFP の中でも企業のオフィス環境で利用される機種で、高度な情報セキュリティ機能を持つ MFP 製品を対象にしている。このような MFP 製品は、日本語の製品カタログでは機能別に「デジタル複合機」、「カラー複合機」または「モノクロ複合機」と呼ばれたり、単に「複合機」と呼ばれたりしている。本書では英語の略称である MFP と表記する。

1.2 本書の背景

日本は MFP に関して、世界的な供給元である複数のベンダーを有している。各 MFP ベンダーは MFP の情報セキュリティに対する要求の高まりから、情報セキュリティ品質の向上を重視しており、IPA が運営する「IT セキュリティ評価及び認証制度」において、数多くのセキュリティ評価の実績を持っている。MFP は「IT セキュリティ評価及び認証制度」において、認証製品件数の約 6 割を占め、セキュリティ機能を備えた IT 製品としては日本を代表する製品となっている。

ネットワーク技術の進展や IT の普及により、MFP はコピーやプリントといった基本的な機能に加え、Web ブラウザによる管理機能、ネットワーク対応、無線 LAN 対応など、基本機能を便利に使うための多機能化・高度化が進んでいる。そのため、製品の安全な使用のための情報セキュリティ面でも、既知の脆弱性の影響のあるプラットフォームを使うことによるリスクや、ネットワーク接続に起因する脅威など、設計段階から多岐にわたる脅威への対抗を考慮しなければならない。開発者が予想しなかった利用形態や設計段階での見落としなど、潜在的な問題点が脆弱性として後から認知され、あるいは設置条件や、機密情報の管理体制が整っていないなどといった運用上の問題点も十分脆弱性となりうる。

1.3 本書の目的

本調査では、上記「1.2 本書の背景」で記載したようなMFPのセキュリティ要件に対する脆弱性について網羅的に洗い出し、どのような攻撃があり、どの程度の攻撃能力により、どの程度の損害となる恐れがあるのか、また、そのための対策としてはどのようなことが有効と考えられるか、多角的な調査を行うものである。

各ベンダーの開発プロセスにおけるセキュリティ確保への取組みや、動作環境における課題や利用者の誤使用といった問題への対処法、MFP の一般的な機能において疑われる脆弱性に講じる対策、それらに対するセキュリティ評価などにおいて本調査を活用することにより、「IT セキュリティ評価及び認証制度」の水準が向上することを目的とする。

1.4 対象とする読者

本調査報告書では主に MFP 製品の企画・設計・開発を行う方と、MFP を利用する方、MFP のセキュリティ機能を評価する方向けに記述している。

1.5 本書の前提と範囲

本調査では、個別製品の詳細な検討ではなく、製品のカテゴリとしての MFP 全体にわたる脅威と脆弱性の可能性の検討を行う。そのため、機能ブロックは概要的な機能のレベルまでの検討にとどめ、個別製品を実現するための詳細な機能ブロックの検討までは行っていない。

利用条件としては、MFP を設置する環境はファイアウォールなどで閉じられたネットワーク内のオフィス用途とし、コンビニエンスストアなどの不特定多数が利用する環境は対象外とする。また、本調査では、オフィスで MFP を利用する環境では情報セキュリティを維持するためのセキュリティポリシが定義され、この方針に従って運用されているものとする。

2. 調査分析手法

本資料ではMFPに関する脆弱性を網羅的に抽出するため、下の図 2-1のような調査分析手法で進める。左から、「1.機能・用途」の特定、「2.機能分担」、「3.保護の対象」の特定、「4.脅威と脆弱性の分析」から、最終的な成果として図の右側にある「5.想定される脆弱性リスト」と「6.MFP独特の脆弱性詳細解説」を作成した。MFPに独特な脆弱性の詳細解説は、想定される脆弱性リストの一部から抽出した、一部の脆弱性を、構成図や背景、原因について詳細に解説したものである。

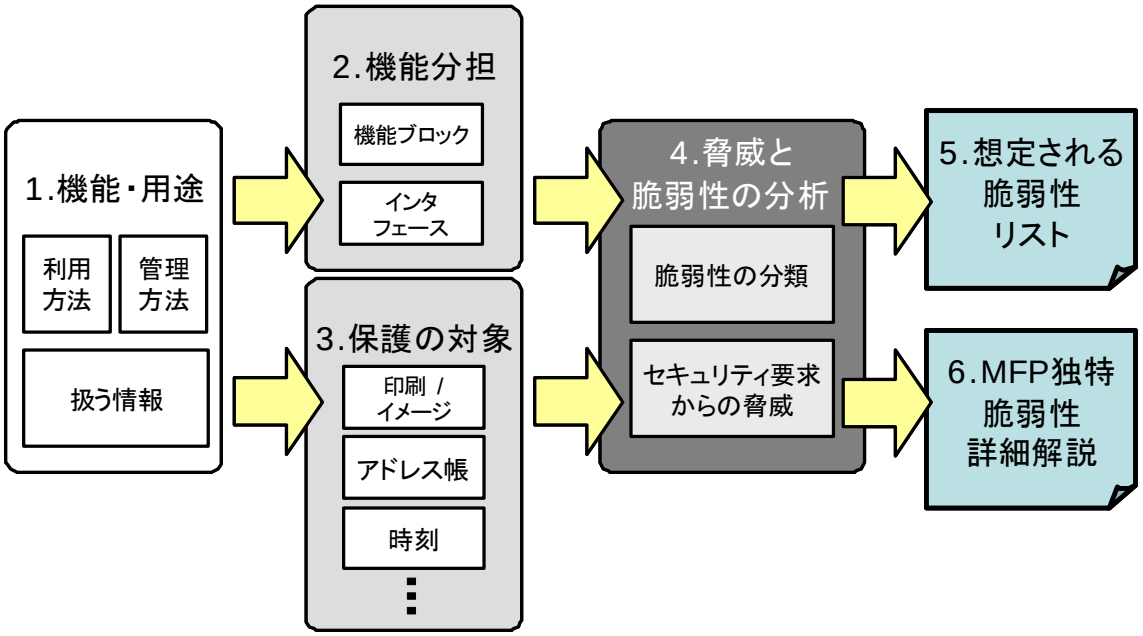

図 2-1 調査分析手法の概要

本調査の手順では、MFPの利用環境における情報システム上の脅威の一覧を特定する。脅威の一覧は、IPA「セキュア・プログラミング講座」で「脅威の洗い出し手順」として紹介されている「脅威モデリング」の手順[1]に従って進める。脅威モデリングでは、システム構成図からデータフローを特定し、インタフェースなどの境界をたどりながら脅威の洗い出しを行う。

本調査では、システム構成図を特定するために、図中左の「1.機能・用途」でMFPの用途と機能を整理した。次に「2.機能分担」でMFP内部と外部のシステム上の機能分担を特定している。また、「3.保護の対象」で情報資産を一次資産から二次資産へと順に特定する作業を行うためMFPの用途に従ってデータフローを整理している。「4.脅威と脆弱性の分析」では、一般的な情報セキュリティへの要求事項として、情報セキュリティマネジメントの標準であるISO/IEC 27001[2]の機密性、完全性、可用性の 3 つと、オプションとして定義されている 4 つの要求事項(真正

[1] 脅威モデリング - IPA「セキュア・プログラミング講座」脅威モデリング
http://www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/c101.html
「脅威モデル～セキュアなアプリケーション構築」Frank Swiderski ほか著、渡部 洋子訳、日経 BP 出版センター、2005 年

[2] ISO/IEC 27001 - 対応する日本工業規格はJIS Q 27001:2006
http://www.isms.jipdec.jp/doc/JIP-ISMS111-21.pdf

性、責任追跡性、否認防止、信頼性)をあてはめて、この要件を破ることが脅威であると想定して脅威の洗い出しを行った。

本調査では「4.脅威と脆弱性の分析」で、脅威の一覧から攻撃手法の例を想定しながら、特に網羅的に脆弱性を抽出することを目的としている。その際、脅威の一覧に対して、どのような脆弱性があてはまるか想定しやすいよう、CWE 共通脆弱性タイプ一覧[3]を参考に利用した。CWE 共通脆弱性タイプ一覧とは、JPCERT[4]とIPAが提供する脆弱性データベース「JVN[5]」など、脆弱性情報を扱う機関で採用が進んでいる脆弱性の分類体系である。CWEには既知の脆弱性の多くが発生原因をもとに階層的に分類されており網羅性が高い。

また「8. 脆弱性の詳細解説」以降で取り上げる詳細解説の一部については、具体性を確保するためMFPベンダー関係者にヒアリングを行った部分もある。

なお、複合機・プリンタが備えるべきセキュリティ機能の国際的な標準規格「IEEE 2600.1[6]」で想定される脆弱性については本調査が包含しているものと考えられる。その理由として、本調査はIEEE 2600.1 で定義するMFP(IEEE 2600.1 ではMFD)の用途を包含しており、さらに本調査ではIEEE 2600.1 で求められる厳しい運用基準に比べ、トレーニング不足による問題、表示のわかりにくさと操作間違い、MFP以外のシステムへのマルウェアの侵入などについても想定しているためである。

2.1 MFPの用途と機能を整理

日本国内のMFPメーカ主要 5 社から一般公開されている「複合機」のうち、ITセキュリティ評価及び認証制度の認証を取得している機種のカタログから用途と機能を特定し、「3.1 MFPの発展の経緯」から「3.6 利用者環境でのMFPの各システムの用途」までに整理した。

2.2 機能ブロックの整理

ITセキュリティ評価及び認証制度で一般公開されている情報からMFPで利用されていると考えられる機能ブロックを特定した。機能ブロックの整理は「3.7 MFPのシステム構成例」から「3.9 MFP内部のソフトウェア」までで行っている。

2.3 守るべき資産として機能ブロック間で交換されるデータを特定

MFP の利用環境で守るべき資産を特定するため、ハードウェアの機能ブロックの間、ソフトウェアの主要ブロックの間で交換されるデータを特定する。このうち、MFP の利用者が直接扱う資産としての一次資産と、一次資産が具体的な媒体

[3] CWE共通脆弱性タイプ一覧 - http://www.ipa.go.jp/security/vuln/CWE.html

[4] JPCERT - JPCERTコーディネーションセンター - http://www.jpcert.or.jp/
インターネットからの侵入やサービス妨害などの被害情報受付と事後対策の支援、調整を行う機関

[5] JVN – Japan Vulnerability Database - http://jvn.jp/
日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供するサイト。

[6] IEEE 2600.1: Hardcopy Device and System Security
Standard for a Protection Profile in Operational Environment A
http://standards.ieee.org/getieee/2600/

に記録された状態や、MFP という情報システムを利用するために副次的に関連する処理データやセキュリティ制御情報などの二次資産を分離しておく。

一次資産と二次資産の整理は「5 MFPの守るべき資産」で行っている。

2.4 脆弱性の分類

ここまでで、脆弱性を網羅できるよう、利用者の通常の用途を網羅するように進めてきた。その一方で、既存のよく知られた脆弱性の分類から見た網羅性を確保するため、既知の脆弱性の分類をあてはめながら、それぞれの脅威が現実に攻撃されるとしたらどの脆弱性が該当するかを検討し、漏れがないようにした。

本調査で利用した脆弱性の分類については「6 脆弱性の分類」で整理している。

2.5 各資産に対して脅威と脆弱性を列挙

一次資産が具体的な情報や媒体となっている状態の二次資産のすべてについて、一般的なセキュリティの要求事項 7 項目をあてはめながら、脅威を列挙する。また、それぞれ列挙された脅威について、その脅威がどのような攻撃や事故などで具体化するか例を挙げながら、原因となると考えられる脆弱性を想定例として列挙する。

これら脅威の一覧と、対応する攻撃例、想定される脆弱性は「7 脅威から想定される脆弱性」に表形式で掲載している。

3. MFP の用途、機能

3.1　MFPの発展の経緯

MFPは日々進化しており、さまざまな利用方法が開拓されている。下の図 3-1は、これまでのMFPの発展の経緯と、今後予想されるMFPの利用想定例を左から順に列挙したものである。

MFP は本来、コピーを中心とした「イメージング」処理を行う装置であったが、これにファクスが統合され、電子化されたイメージデータを転送する機能とネットワーク機能が加わり、飛躍的に機能が増大した。その後、ネットワークを経由して MFP を複数利用者が共有する「遠隔共有」や、MFP を既存の業務システムなどと連携させる「アプリ拡張」などの機能が加わり、MFP への信頼性やセキュリティへの要求も増大するようになった。

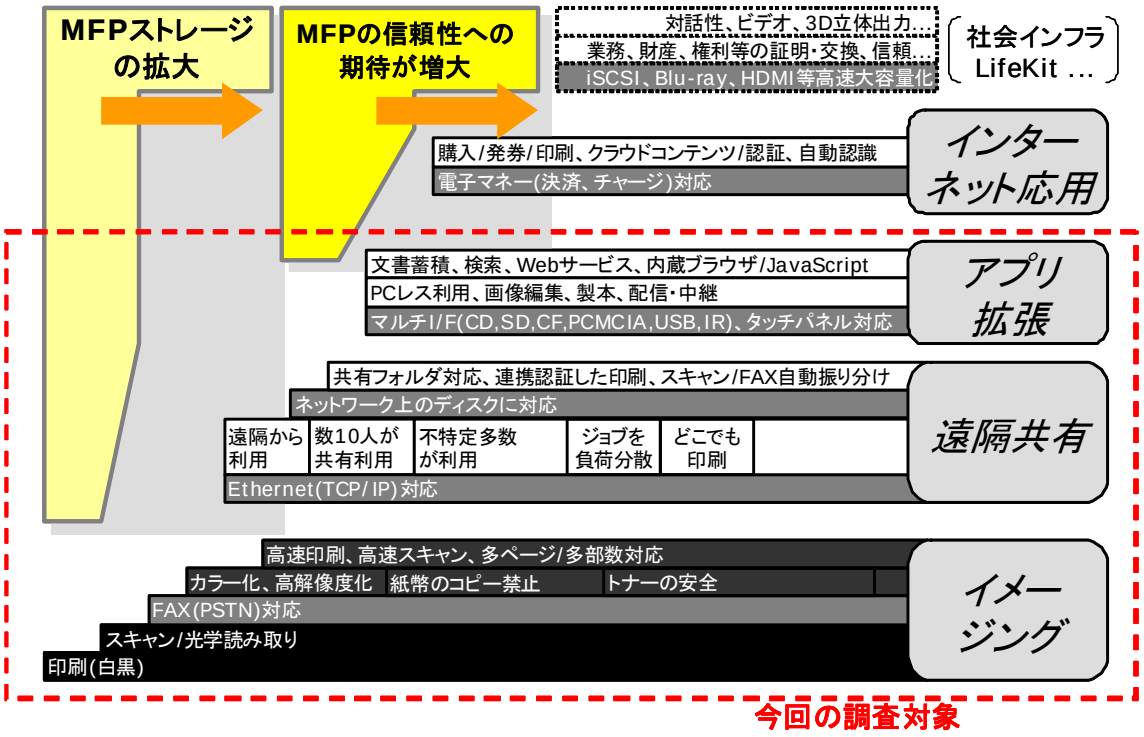

図 3-1 MFP の発展の経緯

図 3-1の右上にある黒い点線の枠内は、将来MFPが機能拡張する可能性を、社会インフラの一部としての役割や、生活小道具(Life Kit)的な面も含めて想定した例である。また、「インターネット応用」は、MFPをインターネット上のサービスやクラウドサービスなどと連携させ、さらに多数の用途で活用するという方向がある。ただし「インターネット応用」については企業のオフィス環境で利用されるMFPについては、対応はごく一部であり、今後発展が期待される分野である。

本調査では現在、企業のオフィス環境で利用されるMFPに一般的に普及している機能を調査対象とし、ごく一部の機種だけの機能や将来の機能については対象外としている。そのため、本調査では図 3-1の赤い点線の枠内で示した範囲を対象として調査検討を行った。

3.2　MFPに求められるセキュリティ

下の図 3-2ではMFPの進化の方向にあると考えられる、MFPに求められるセキュリティの一例である。ただし、MFPには非常に多数の機能が実装されているため、網羅的な脆弱性の特定が必要だと考えられる。そのため、本資料ではMFPの本来必要とする用途や機能から順に、MFPの利用環境での脅威と脆弱性を抽出するものとする。

なお、下の図 3-2のうち、本調査で対象としているのは図の下にある「イメージング」から上に「アプリ拡張」までとなっている。「インターネット応用」については一部の機種でMFP内部に機能を搭載していたり、MFPの外部のシステムとして提供されたりしているが、MFP内部の機能として普及しているとは言えないため除外した。

機能カテゴリ	機能例	想定される脅威と対策例
インターネット応用	・検索/インデックス付与サービス ・文字/意味識別、分類サービス ・決済/証明サービス	▼脅威：ランク付けされたインデックス情報、アクセスログの漏洩 ▼対策：インデックスを含めた暗号化HDD運用、など
アプリ拡張	・サードパーティによる拡張アプリ ・特定文書の判定/識別 ・オープン認証/セキュリティ高度化	▼脅威：拡張アプリの実装間違いによる必須認証の欠如と脅威 ▼対策：MFP基盤とセキュリティのフレームワーク化と普及促進
遠隔共有	・高速化、ファイルと機能の共有 ・地域単位での多人数での共有 ・IPv4アドレス枯渇への対応	▼脅威：USBを遠隔にブリッジしたとき、予想外の場所で印刷ジョブが盗聴される ▼対策：USBをブリッジするときはプリンタドライバ通信の暗号化か、通信路暗号化を適用する
イメージング	・高解像度、高速化 ・高速な暗号化、署名	▼脅威：高解像度と高速化のため暗号化運用がしにくい、暗号化をオフにして運用する ▼対策：ネットワーク分離・隔離/外部暗号化高速処理に対応した暗号化モジュールやHW機能(IP)の利用

図 3-2 MFP に求められる機能、セキュリティ

図 3-2の「インターネット応用」は、MFPの内蔵機能だけではなくインターネットやネットワーク上にあるさまざまな機能を応用する方向性を指す。例えばMFP内部に共有できるように蓄積された文書を高速に検索するためにインデックスを付与するサービスとの連携がある。また、スキャンした画像から文字を抽出して検索しやすくする機能や、写真画像から顔を検出し、自動的に分類する機能などがある。また、現金だけではなく電子マネーも含めた料金の決済機能との連携で、MFPを利用したコンテンツ販売機能や、住民票などの証明書の印刷機能を持つMFPもある。

インターネット応用については検索に必要なインデックス情報自体も文書の内容と同じような情報を格納していることから、間接的に MFP の利用環境における脅威と考えられる。ただし、インターネット応用については MFP に一般的な機能とは見られなかったため、今回の調査対象としていない。

「アプリ拡張」については、MFP メーカ以外のサードパーティが開発したソフトウェアによる拡張アプリによって、さまざまな機能が利用できる特徴がある。特定の専用型式のファイルの処理や、外部の認証機能との連携機能などがある。認証については既存の単機能を対象にした認証手順だけではなく、複数の機能で利用できるオープンな認証手順がある。こうしたオープンな認証手順ではセッション情報の維持や、なりすましのセッション情報の再利用などの脅威への対策が必要だが、オープンであるため管理が複雑になる。そのためセッション情報の管理機能を統合的に提供する開発フレームワークの採用などの対策が必要になる。

「遠隔共有」ではネットワークの高速化により、遠隔地との高速なファイル共有や機能の共有がさらに使いやすくなっている。ファイル共有だけではなく、プリント機能を USB デバイスとして遠隔地で共有する機能もある。また、遠隔共有を支えるネットワークは TCP/IP を使って国単位や地域単位での広がりを持って利用されている。TCP/IP については現在、IPv4 というプロトコルが主に利用されているが、IPv4 アドレスは 2011 年以降段階的に枯渇するとも言われている。IPv4 アドレスの枯渇対策としては通信事業者による IPv4 NAT の対応や、通信事業者と製品の両面で IPv6 プロトコルへの対応が進められている。MFP については特に IPv6 プロトコルへの対応がもっとも進んだ IT 製品のひとつとなっている。

「イメージング」では、MFP の基本機能であるコピー、プリント、スキャン、ファクスのための画像処理と印刷、読み取りの高解像度化、高速化がある。画素数の増大、色の深さの増大、紙送りと印字速度の高速化が一体となって進んでいる。こうした高速化に対応して、暗号処理などのセキュリティ対策も相当の高速化が行われている。

3.3 MFPを利用する環境でのライフサイクル

下の図 3-3は、MFPの利用者から見た、MFPの利用計画から廃棄までのライフサイクルを示している。本調査では製品に関する一般的なライフサイクルのうち、「設置」「運用」「廃棄」のフェーズのみを対象としている。主に図の左側に利用者自身が行うもの、図の右側にメーカや専門業者など、外部に委託することが多いと考えられる作業を整理した。

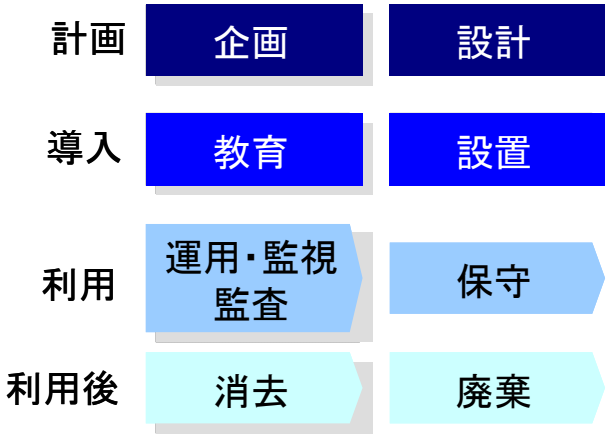

図 3-3 MFP を利用する環境でのライフサイクル

3.3.1 計画

「計画」は、利用者が MFP を利用する目的や得たい効果を検討する段階を指す。MFP 利用目的には、例えば「MFP を利用して文書取り出しを容易にわかりやすくする」、「業務手順を短縮しながら文書交換の安全性を高める」「必要な業務や作業の記録を自動化して効率化・確実化する」などがあるだろう。目標に従って、得たい効果を実現するためのしくみや利用方法の特定を行うことが、「設計」にあたる。

また、企画・設計の過程で、守るべき資産と、確保が必要な安全性の基準、その具体的な対策方針も検討する。安全性の基準と対策方法はセキュリティポリシとして、一般的には MFP を含む利用者の情報システム全体として規定されるが、MFP の利用環境については、一部のセキュリティポリシを追加・変更する場合がある。

3.3.2 導入

「導入」には、MFP 利用者への教育と、MFP 機材の設置がある。MFP 利用者への教育では、MFP 上での文書の取り扱い方や、認証方法、操作がわからないときの問い合わせ先などが一般利用者に周知される。運用者や保守者に対しても、特定の MFP 機種に関する構成・設定方法や、MFP 動作の監視・確認方法、故障時の対応方法などのトレーニングが行われる。

MFP 機材の設置では、機材を所定の場所に適切に配置し、所定のソフトウェアの投入や初期設定を行う。また、関連システムとの配線を行って、連携した動作の確認を行う。

3.3.3 利用

「利用」フェーズでは、MFP を利用する現場で主に行う作業として「運用・監視」と「監査」、MFP を利用する現場とは異なるメーカや保守専門業者などが行う作業として「保守」に分けている。

「運用」には、管理者が MFP の設定を変更する作業のほか、一般利用者による MFP の利用も含めている。MFP の監視については、MFP の利用形態が一般的には利用者のサイト内で閉じたネットワーク内で運用されることが前提となっている

ため、利用者寄りの作業として位置づけている。
「監査」では、稼働量の情報や運用中のインシデントなどの記録から、適正な運用が行われていたかどうか、その結果対策として何をするべきか検討する。
「保守」では、MFP 本体の故障修理や、部品またはソフトウェアの追加変更などの作業がある。

3.3.4 利用後

「利用後」には「消去」と「廃棄」の作業がある。利用後には、利用者は廃棄に備えてデータや設定情報の「消去」を行う。「廃棄」では、利用しなくなった MFP を廃棄業者や中古業者に回収してもらうときに何をすべきかなどを含む。

3.4 情報システムから見たMFP

下の図 3-4はMFPを利用する環境を、情報システムとしてみた図である。図の右上のMFPは、図中央の通信システムを介して、図の左上にある利用者端末や図の中央上にある蓄積・外部処理などの他のサービスと連携して動作する。また、図 3-4 の下にある遠隔管理システムは、MFPのコンソールパネルではなく、ほかの端末やサーバからMFPの設定ができる。遠隔管理システムには、MFPの利用者やMFP本体、蓄積・外部処理サービスのそれぞれの認証や許可の機能も持つ。

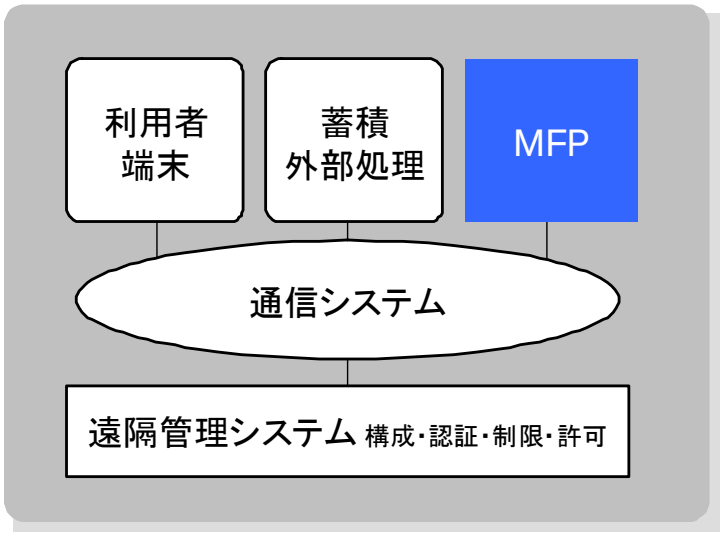

図 3-4 情報システムから見た MFP

3.4.1 利用者端末

「利用者端末」はネットワークや通信システムを経由して MFP を利用する端末を指す。MFP の利用者には、印刷やファクス送信などを行う一般利用者のほか、MFP 本体の構成変更や設定を行う管理者と、一部ソフトウェアの追加や削除などを行う保守者を含む。「端末」の意味は、人が操作と表示を行う点を重視している。

3.4.2 蓄積・外部処理

蓄積・外部処理は、主に MFP 外部のシステムのうち、人が直接操作せず、自動的に機械が処理するシステムをまとめている。MFP の利用環境においては特に文書の長期格納やジョブデータの一時的な保存やスプール処理を行う「蓄積」と、画像処理や文字抽出と業務システムとの連携、文書の検索処理などさまざまな処理を含めて「外部処理」として呼んでいる。

3.4.3 通信システム

「通信システム」は MFP が外部のシステムと通信を行うために MFP の外部にある通信システムを指す。通信システムの中には、Ethernet スイッチや IP ルータとその配線、無線 LAN アクセスポイントなどがある。MFP に USB ハブを経由して接続する場合は、USB ハブと USB ケーブルも含まれる。

「通信システム」は一般的なオフィス向けの MFP の利用形態では、MFP を利用する企業内の LAN や VPN などの、企業内で閉じられたネットワーク内に限定されている。MFP と利用者端末、蓄積・外部処理はすべて企業内に閉じられたネットワークの中で接続されている。なお、企業内に閉じられたネットワークを通称して「内部ネットワーク」と呼ぶこともある。

例外的に、企業外の保守業者が提供する遠隔保守サービスのようにインターネットや企業外のネットワークを経由する場合がある。

なお、ファクス通信のような組織外との通信については、通信システムを経由して他の組織にあるMFPと通信するが、その場合は「3.5 他の組織との間から見たMFPの利用システム」として区別している。

3.4.4 遠隔管理システム

「遠隔管理システム」は通信システム経由で MFP の管理操作を遠隔から行うための MFP の外部のシステムである。構成変更や設定作業、保守作業などを行うために MFP メーカから配布されている専用ソフトウェアや、MFP 内の設定変更を行うときに利用されるブラウザも遠隔管理システムの一部と考えられる。また、図にはないが、遠隔管理システムには、遠隔からの監視や保守の機能も含む。

「遠隔管理システム」は一般的なオフィス向けの MFP の利用形態では、MFP を利用する企業内で閉じられたネットワーク内にある。例外的に企業外の保守業者が提供する遠隔保守サービスのように企業外のネットワークに設置されている場合がある。

3.5　他の組織との間から見たMFPの利用システム

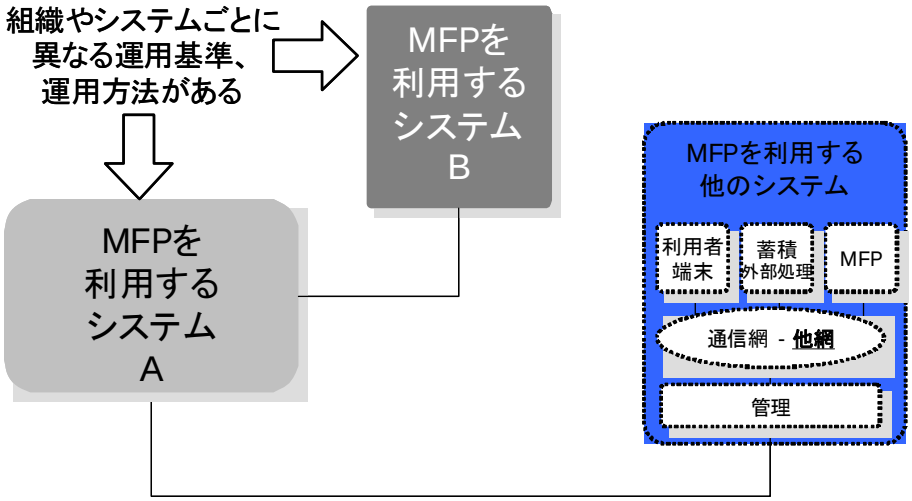

図 3-5 他の組織との間から見た MFP の利用システム

図 3-5はMFPを利用するシステム同士が接続されている関係を示している。MFPのファクス機能を利用する場合でファクスの送受信先が社外である場合、このように組織外との通信を行うことがある。

2 台以上の MFP が同一組織内で利用される場合、各 MFP はほぼ同様の運用方針に従って運用されるが、異なった組織との間では、異なった運用方針によって運用される場合がある。具体的には、ある組織 A はメールサーバへのログインが管理者のみに認められ、ほかの利用者には認めていないが、別のある組織 B では、メールサーバへのログインが誰にでも認められている、などのケースがある。

こうした環境の違いによる影響はファクスの送受信やスキャン後のイメージのファクス転送やメール配信など(スキャン to X)、イメージを転送するときに発生しやすい。

3.6　利用者環境でのMFPの各システムの用途

表 3-1 利用者環境での MFP の各システムの用途

用途カテゴリ	用途	一般利用者から	他のMFP間	他のシステム間	管理者から	保守者から
一般	印刷	○	○	○		
	コピー	○	○			
	スキャン	○				
	ファクス送信	○				
	ファクス受信		○			
	負荷分散印刷		○	○		
	スキャン送信	○				
	配信、伝送	○	○	○		
運用	設定の追加･削除	○			○	
	稼動情報取得				○	
	監視				○	
保守	部品交換と設定、バックアップ					○
	ソフトウェア更新･追加					○
	料金メータ読取、初期化					○
	故障分析、診断					○

上の表 3-1は、利用者環境でのMFPの各システムの用途がそれぞれ存在することを確認する表である。一般利用者と、管理者・保守者からの利用では、それぞれ用途が異なる。大きく分けて管理者と保守者では、印刷、コピー、スキャン、ファクス送受信の用途はない。その逆に、一般利用からの用途に、運用と保守の用途カテゴリ(表左の列)の用途はない。

MFP の一般的な機能である、印刷、コピー、スキャン、ファクス送受信など、文書の複製やデジタル化の機能については、一般利用者が利用する。また、他の MFP との間で、印刷処理を分担したり、ファクスを送受信したりする。さらに、対向するホストが MFP ではなく、共有ファイルサーバや業務システムなどの「他のシステム」である場合がある。

管理者は、MFP の運用を支える役割を持ち、設定の追加・削除、稼動情報の取得、監視などを行う。

保守者は MFP 本体の故障に対応して、部品交換や修理を行う。修理交換の際には、管理者に代わってバックアップを行うことがある。また、MFP 内部のソフトウェアの更新と追加削除、料金メータの読み取り、故障診断を行う。

なお、一般利用者が、その一般利用者自身が利用するためだけの設定を追加変更することがあり、一部限定された機能については一般利用者も設定変更をすることもある。また、MFP 製品では、こうした利用者の役割ごとに機能の利用制限を設定できる。

3.7　MFPのシステム構成例

下の図 3-6はMFPのシステム構成例を示している。中心の青い「MFP」とあるのがMFPである。MFPにはUSBメモリなどのポータブルメディア(以下、着脱式媒体)や、認証用のICカードリーダが接続されることがある。機種によってはあらかじめMFPの本体内に内蔵されている場合がある。

MFP の右下にある「保守者パソコン(端末)」は、保守者が MFP の故障診断を行ったり、バックアップを取り出したりするための端末である。図の左上には、「一般利用者パソコン(端末)」と「管理者パソコン(端末)」がある。一般利用者端末は

内部に MFP 用のドライバ(プリンタスキャナドライバ)をインストールし、MFP と通信をして MFP のサービスを利用する。管理者端末は MFP を遠隔で設定するのに利用される。

図の右下にあるのはファクス機能である。PSTN-FAX(PSTN ファクス)は、既存の電話網を利用したアナログファクスモデムによるイメージ伝送を行う。IP-FAX(IP ファクス)には、メールサーバを使ったメールファクスと、IP アドレスで直接相手の MFP に SMTP 接続する IP ファクス、さらに SIP を利用してファクスのイメージ伝送を行う SIP ファクスがある。

なお、既存のPSTNファクスの場合でも、SIPまたはH.323 手順に変換可能なTA(Terminal Adapter)という装置を利用してIP化する場合もある。TAを利用すると、遠隔地のPSTNファクス間での通信をIPネットワークまたはインターネット経由で中継し、既存のPSTN経由でのファクス通信料金を削減できるメリットがある。図3-6では、図の右下にあるTAで、MFPのPSTNポートをIP化する例を示している。

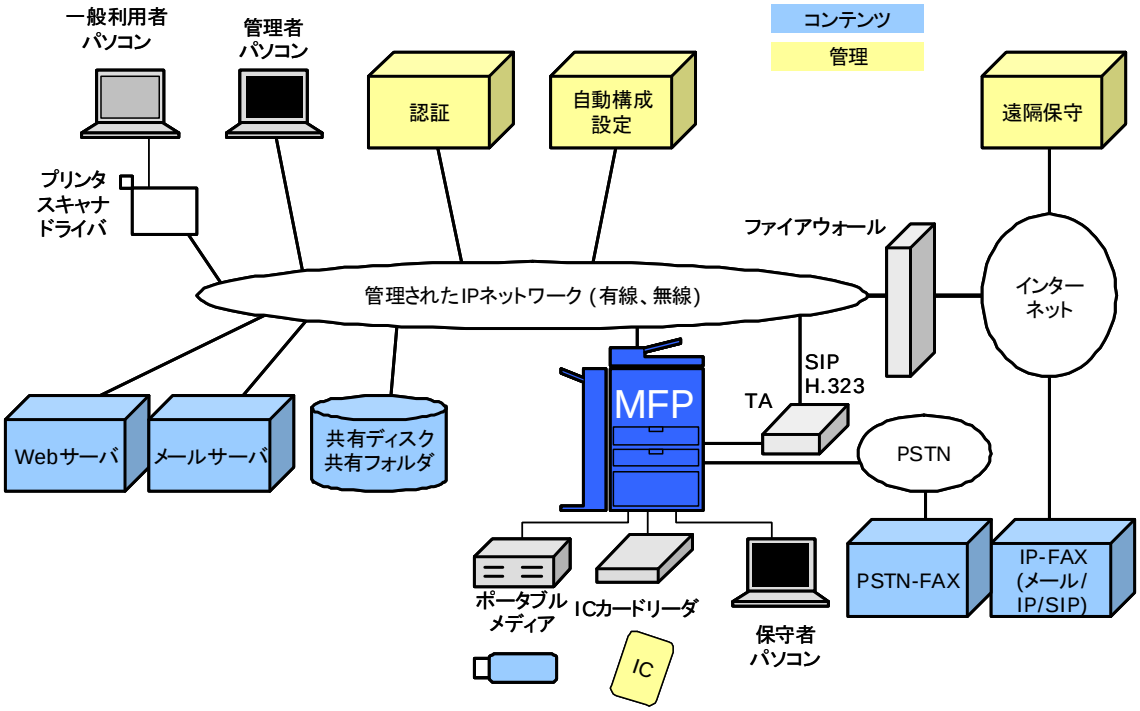

図 3-6 MFP のシステム構成例

MFP のすぐ左にある「共有ディスク 共有フォルダ」は MFP がスキャンしたイメージやファクスで受信したイメージを保存するのによく利用される。その左の「メールサーバ」は、やはりスキャンイメージや受信したファクスのイメージをメールで受信したいときに MFP からイメージが送られる先である。また、MFP 内部での異常や失敗した処理の通知が、このメールサーバを経由して管理者や利用者に送信される場合もある。メールサーバの左の「Web サーバ」は、MFP が内蔵している Web ブラウザを利用して MFP の外部の画像を利用したり、MFP の外部にある業務システムと連携したりするために利用されることがある。

黄色の四角でいちばん左にある「認証」は、ネットワーク上で MFP の外部にあって認証サービスを提供するサーバなどで、シングルサインオン機能を提供することもある。認証の右にある「自動構成 設定」は、MFP を含むネットワーク内で、自動的に IP アドレスを割り当てたり、正しい時刻に同期させたり、MFP の稼動を

監視したりする機能がある。図の右上の「遠隔保守」は、MFP メーカや保守業者による、遠隔地からの MFP の保守サービスである。遠隔保守では、トナーやドラムの寿命の監視、印刷などの利用枚数の監視などを行う。

この例では、特に MFP 用のスプールを行うサーバと、利用者サイト内の監視サーバ、MFP が利用するプロキシサーバについては記述しなかったが、利用者の環境によっては利用されることがある。

3.8 MFP内部のハードウェア

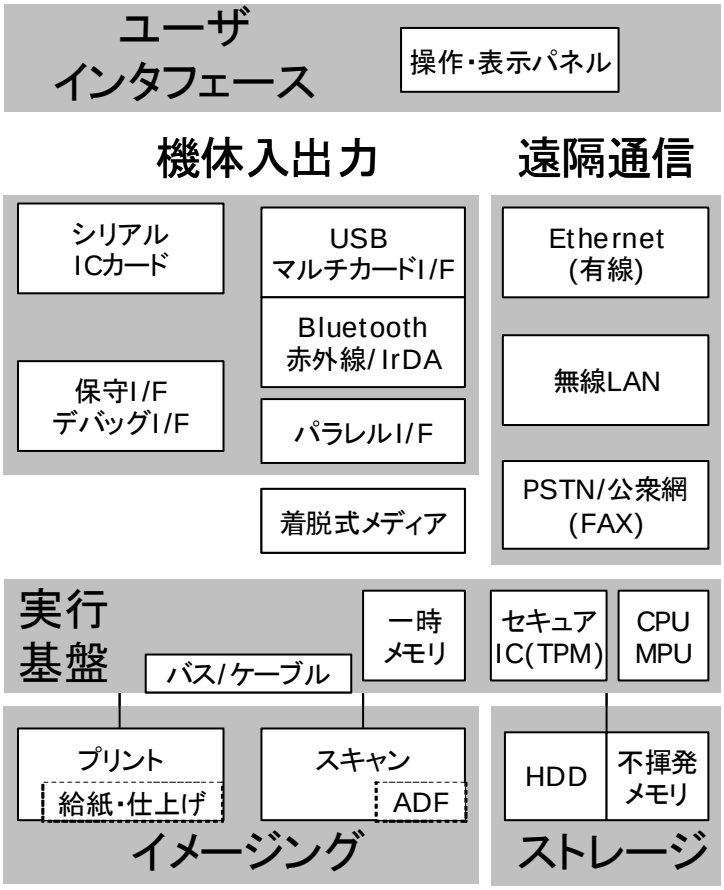

図 3-7 MFP 内部のハードウェア

MFP はプリントとスキャン、ネットワークなどの複数の機能を搭載し、連携して動作させるため、プリント、スキャン、実行基盤などの複数のハードウェアを組み合わせて構成する。

3.8.1 MFP内部のハードウェア - イメージング

プリントには、用紙トレイから用紙を取り出す給紙機構や、内部から外部へと紙を送る機構、イメージを転写して定着させる機構などからなる。また、プリント機能の追加機能として、仕上げ機構がある。仕上げ機構は「フィニッシャ」などと呼ばれる。仕上げ機構には、プリントされた印刷物を部単位でソートしたり、ホチキスで留めたり、印刷物を折ったりする機能がある。

スキャンは原稿に光をあてて、反射光をデジタルデータとして読み取る装置である。原稿を 1 面ずつ読み取るためのガラスなどの読み取り台がある。また、積み重ねられた複数枚の原稿を連続的に読み取るために、ADF(Auto Document Feeder)が装着されている。読み取り台には、読み取り台に置かれた原稿を読み取るための、移動式のスキャナモジュールがある。ADF には、原稿をスキャナに給紙するときに両面で一度に読み込むために、読み取り台とは別のスキャナモジュールを内蔵する機種もある。MFP の場合、高速なスキャン処理を実現するため、ADF 内にスキャナモジュールを内蔵する機種は多いと見られる。

3.8.2 MFP内部のハードウェア – ストレージ

「ストレージ」は、MFP 内部で文書や一時的なジョブデータ、設定値などを保管するために利用される。ストレージ上のデータは利用者のなんらかの操作によって書き換え可能である。

3.8.3 MFP内部のハードウェア - 機体入出力

「機体入出力」は、本資料中で独自に、MFP 本体と対向で通信するインタフェースを抽出してまとめた呼び名である。主なものは、USB マルチカードインタフェースで、USB メモリや SD カードメモリ、CF カードなどの複数の着脱式媒体を装着できるユニットのインタフェースである。また、Bluetooth や赤外線(IrDA)インタフェースも、ほぼ MFP と対向で接続するものと考えられる。パラレルインタフェースとは、古くからあるプリンタ中心に用いられたインタフェースで、パソコン本体にも装備されていた。

「機体入出力」にはその他、認証用のインタフェースと、保守/デバッグ用のインタフェースがある。

認証用として MFP のコンソールを操作する利用者を認証するための IC カード認証装置や生体認証用のインタフェースがある。

保守インタフェースとしては、MFP 本体の保守時に MFP の故障診断を行う機能がある。また、デバッグインタフェースは製品には残っていないと考えられるが、MFP 製品を開発するときに、実行基盤上のソフトウェアの状態を確認・変更したり、書き換えたりすることができるインタフェースである。デバッグインタフェースは CPU の実行レベルで制御を行うため、MFP 内部に設定された権限や制限などの制約からは一切影響を受けずに動作する。

3.8.4 MFP内部のハードウェア - 遠隔通信

遠隔通信は、MFP から多段の通信機器などを経由して通信するインタフェースを、本資料中で独自にまとめた呼び名である。Ethernet や無線 LAN、PSTN 公衆網(PHS を含む)がこれにあたる。これらの通信インタフェースは、ルータやスイッチ、交換機などを通じて全世界とグローバルに通信することができる。遠隔通信はグローバルなインタフェースとすれば、機体入出力は MFP 周辺のローカルなインタフェースともいえる。

3.8.5 MFP内部のハードウェア - ユーザインタフェース

MFP の「ユーザインタフェース」は、MFP の表示用の液晶画面と、キーボードを含むコンソールパネル(略してコンソール)がある。コンソールが MFP 本体に組

み込まれている MFP のほか、一部機種ではコンソールが外部に分離され、大型化されているものもある。

3.8.6 MFP内部のハードウェア - 実行基盤

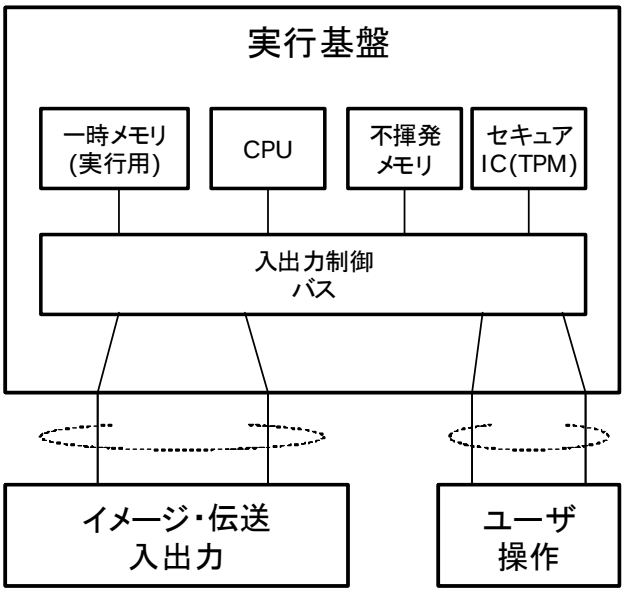

図 3-8 MFP 内部のハードウェア - 実行基盤と主なインタフェース

図 3-8 は MFP 内部のハードウェアの実行基盤と主なインタフェースを示す。「一時メモリ(実行用)」は DRAM(Dynamic Random Access Memory)などで提供される、ソフトウェアの実行時に利用される、揮発性のメモリを指す。「CPU」はソフトウェアを実行するための演算処理を行う。「不揮発メモリ」は実行用のソフトウェアや、実行用の設定値を保管するために利用される。「セキュア IC(TPM)」は、内部に暗号処理用の秘密鍵を持ち、暗号処理が可能な IC である。セキュア IC(TPM: Trusted Platform Module)は暗号処理を行う際に、秘密鍵をセキュア IC 外部に取り出す必要がなく、安全に秘密鍵を保管できる特徴を持つ。

3.8.7 MFP内部のハードウェア – モジュール間の接続

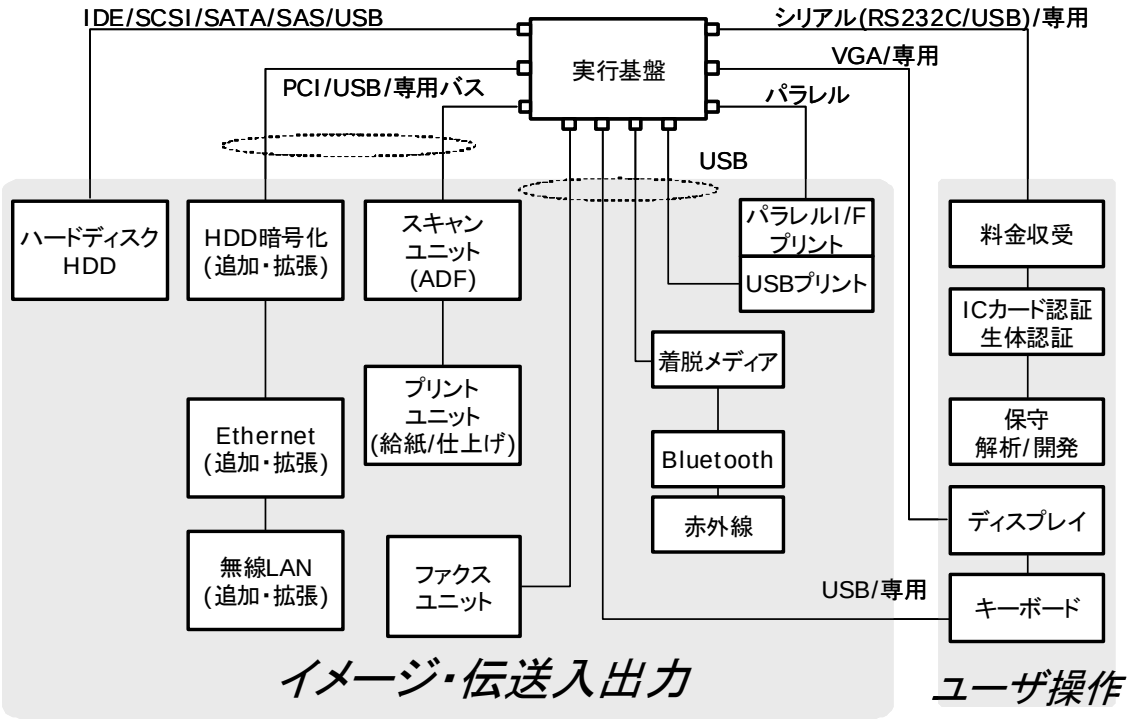

図 3-9 MFP 内部のハードウェア - ユニットまたはモジュール間の接続

上の図 3-9はMFP内部のハードウェアのうち、実行基盤とそれ以外のハードウェアが接続される構成を示したものである。

図の左、ハードディスク用の標準インタフェースとしては、IDE/SCSI/SATA/SAS/USB などがある。IDE(Integrated Drive Electronics)はパソコン用によく普及した安価なインタフェースだが、ケーブルの配線本数が多く、コネクタが大きくなるデメリットがある。SCSI(Small Computer System Interface)はハードディスクに限らずスキャナなども複数台接続できるメリットがあるが、IDE と同じくケーブルの配線本数が多い。SATA(Serial Advanced Technology Attachment)はケーブルの配線本数を大幅に減らしながら、IDE よりも高速な転送が可能で、安価に提供されている。ハードディスク用インタフェースには SAS(Serial Attached SCSI)というインタフェースも標準化されているが、一般的に高価である。USB はハードディスクへのインタフェースとして利用されることもあるが、転送速度を確保しにくい場合がある。

図 3-9の左から二列目のHDD暗号化はハードディスクに書き込み/読み出しするデータを暗号化/復号する機能である。MFPではオプションとして提供されることが多い。「Ethernet」と「無線LAN」は、実行基盤上で提供される場合もあるが、実行基盤とは別のモジュールを追加する形で提供される場合もある。これらHDD暗号化モジュールやEthernetモジュールは高速なデータ転送が必要であるのと、モジュール自体は小型にできるため、PCI(Peripheral Components Interconnect)バスやUSBバス、またはメーカ独自の専用インタフェースで提供される。

スキャンユニットとプリントユニットは、MFP のイメージ処理の中核にあたるため、実行基盤との間では PCI バスなどの高速インタフェースのほか、メーカ独

自の専用インタフェースが利用される。また、印刷イメージの展開や、読み取り画像の加工などのイメージ処理機能がスキャンユニットやプリントユニットの側に装備されている場合もある。

ファクスユニットよりも右の列にあるモジュールは、より低速なインタフェースである。ファクスユニットの主な用途はモノクロで、カラー画像のイメージ転送も行う場合でも、ファクスイメージの伝送のリアルタイム性はあまり重要視されていない。また、ファクス機能自体がオプション機能として扱われることがよくあるため、USB などの汎用インタフェースで接続されることもある。

ファクスユニットの右にある、「着脱メディア」は USB メモリや SD カードなどの着脱できるメディア用のモジュールである。MFP に対してデジタルカメラの画像をメディアの抜き差しによって投入できる。「Bluetooth」と「赤外線」は携帯電話やデジタルカメラなどと近距離で通信し、MFP にプリント画像を投入できる無線のインタフェースである。同じ無線 LAN との間の違いは、Bluetooth や赤外線は別のネットワークを広域に接続せず、MFP の周辺に限って接続できる点である。Bluetooth の場合は最大で半径約 10m、赤外線は間に光をさえぎるものがない状態で最大数 10cm 程度である。

図のいちばん右側下の、「ディスプレイ」と「キーボード」は、MFP 本体に装備されている表示用のコンソールパネルと、操作用のキーボードを指す。一部機種では MFP の本体外に独立した表示装置やキーボードを持つ。

図の右上にある「料金収受」は、公衆向けの MFP などで料金として貨幣を投入して利用するための装置である。「IC カード認証・生体認証」は、MFP の利用者を識別するために、非接触 IC カードや指紋などの生体情報を使って認証を行うモジュールである。IC カード認証・生体認証と MFP 実行基盤の間は RS232C や USB などで接続されている。「保守/解析/開発」は MFP の故障時に故障原因を詳細に調べたり、一部の設定やソフトウェアを更新したりするために利用される。ただし、開発インタフェースは通常は利用者にとっては用途がないため、製品内では削除しておくか、無効にしておく。

なお、本資料では「料金収受」については利用シーンが「閉じた企業内」という想定と異なるため、検討は行っていない。

3.9　MFP内部のソフトウェア

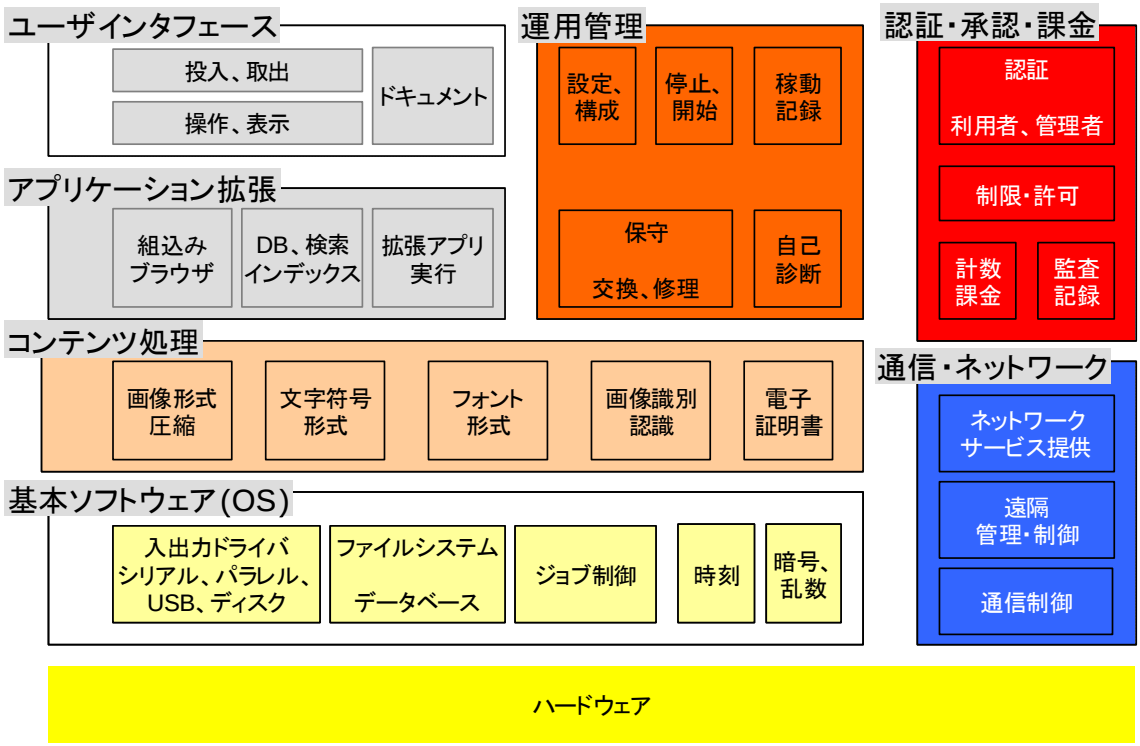

図 3-10 MFP 内部のソフトウェア

MFP のハードウェア上で実行される、MFP 内部のソフトウェアについて機能ブロックを整理した。以下に、各機能ブロックの内容について説明する。

3.9.1　ユーザインタフェース – 投入、取出

ユーザインタフェースの「投入、取出」は、紙としての原稿や印刷物の投入と取り出しを指している。

ネットワーク経由でのジョブデータの投入と取り出しについては通信・ネットワークの「ネットワークサービス提供」としている。

3.9.2　ユーザインタフェース – 操作、表示

ユーザインタフェースの「操作・表示」は、MFP 本体のコンソールやキーボードを使った操作・表示を指している。必要があれば本体上に貼られたシールなどで示された操作ガイドやマークなども含む。

3.9.3　ユーザインタフェース – ドキュメント

ユーザインタフェースの「ドキュメント」は取扱説明書やマニュアルなど、MFP の使い方を説明した資料のことを指す。MFP で動作する機能の使い方がすべて記載されたものである。

3.9.4 アプリケーション拡張 – 組込みブラウザ

アプリケーション拡張の「組込みブラウザ」は、MFP 内部に組み込まれた Web ブラウザを指す。組込みブラウザは所定の処理に従って、MFP の外部の Web サーバや Web サービスに対して要求を行い、パソコン用の Web ブラウザのように、Web サーバから応答として受信した HTML ファイルの解釈や JavaScript の実行を行い、必要な情報を得る。

組込みブラウザの利用例としては、外部の業務システムで動作する Web サーバに業務や印刷用のデータの要求する、などがある。

3.9.5 アプリケーション拡張 – DB、検索インデックス

「DB」は MFP 内で利用されるデータベースである。多数のアドレスや、MFP 内のボックスや共有文書として格納さるファイル、長時間にわたるジョブデータなどを管理するために利用される場合がある。DB については汎用的な SQL 言語インタフェースを持つデータベースが利用される場合もある。ただし SQL 言語インタフェースについては、インターネットの Web と DB を利用したシステムで SQL インジェクションなどの攻撃事例が多数発生しているため、MFP においても配慮が求められるところである。

「検索インデックス」は MFP 内に保管された文書ファイルを全文検索するために利用されるインデックス情報のことである。

全文検索では、1 つ以上の単語をもとに、高速で多数のファイルを検索するため、事前に単語単位で文書ファイルを指し示すよう整理されたデータとして検索インデックスを用意する。そのため、検索インデックスには、多数の文書から抽出された単語と、その出現頻度や含まれる文書ファイル名などが含まれている。

また、検索インデックスのデータ量はほぼ元の文書の大きさと同等かそれ以上と、大きくなりがちなため、複数のユーザ間で共有するのが一般的である。しかし、文書によっては特定の利用者にのみ閲覧や書き込みを許可するなどのアクセス制御が必要なため、検索インデックスの扱いには注意が必要である。

3.9.6 アプリケーション拡張 - 拡張アプリ実行

「拡張アプリ実行」は、MFP上で、そのMFPメーカではないサードパーティの開発者や利用者が開発したソフトウェアを実行できるようにする機能のことを指す。拡張アプリ実行では、Javaで開発したアプリケーションを実行[7]させたり、そのMFP用に開発した特定の命令をMFP内部のブラウザに実行させ[8]たりすることがある。

また、各 MFP 用に拡張アプリを開発するための環境として、MFP メーカでは「SDK (Software Development Kit)」と呼ばれる開発環境を配布している。一般的に SDK では、特定メーカや特定機種が提供している MFP 上のサービスや MFP 用の

---

[7] RICOH Developers Challenge - 「Java で複合機を駆使する」
http://www.ricoh.co.jp/javachallenge/outline/
Canon MEAP - 「Java技術によってOS非依存」
http://web.canon.jp/technology/canon_tech/explanation/meap.html

[8] FujiXerox Apeos IntegrationPlus
http://www.fujixerox.co.jp/solution/dsp/product/integrationplus/index.html
KonicaMinolta OpenAPI
http://en.wikipedia.org/wiki/Konica_Minolta_OpenAPI

ドライバの機能を他のソフトウェアから呼び出せるよう、ライブラリや呼び出し仕様(API: Application Programming Interface)が提供されている。

SDK を利用すれば、MFP のメーカではない第三者が新しいソフトウェアを開発し、MFP の機能をさらに拡張したり、別のシステムと連携動作させたりすることができる。また、SDK には、MFP の外部で動作するソフトウェアを前提にしたものと、MFP の内部に追加して実行させる前提のものがある。

3.9.7 コンテンツ処理 - 画像形式・圧縮

MFP では紙にプリントをするために、MFP ごとにあらかじめ決められた形式の画像を受信して処理し、紙に転写する処理を行っている。そのため、MFP 内部では特定の画像形式のデータを高速に扱う機能がある。また、MFP は一般的に JPEG や TIFF、PDF などの特定の画像形式や画像圧縮形式を利用したファイルを直接取り込んで展開するなどの処理ができる。

3.9.8 コンテンツ処理 - 文字符号形式

一般に MFP はビットマップ化された画像データをもとに印刷処理しているが、PDF または PostScript のように、文字コードを受信して、MFP 上に搭載されているフォントを独自に展開してプリントイメージを生成する場合がある。その際、文字の符号形式(文字コード)への対応が必要となる。日本語では JIS、SJIS、EUC、Unicode など複数の文字コードが存在し、それぞれはマルチバイト文字コードと呼ばれ、1 文字につき 2 バイト以上の長さを持つ。

3.9.9 コンテンツ処理 – フォント形式

PDF または PostScript のように MFP 内で文字コードから文字のイメージを展開するためには、文字ごとに字の形を定義した「フォント」というデータが必要になる。MFP がフォントを展開するには、特定のフォント形式に対応した処理が必要である。PDF または PostScript 用には、PostScript フォントが MFP メーカから提供されている。

3.9.10 コンテンツ処理 - 画像識別・認識

MFP の一部の機種では、MFP 内部でスキャンした画像やファクス受信した画像から、画像内の文字を識別・認識する機能を持つものもある。ただしこの機能は MFP 一般に内蔵されている機能ではないため対象外とする。

3.9.11 コンテンツ処理 – 電子証明書

MFP の一部の機種では、MFP 内部でスキャンした画像や、MFP に登録した電子ファイルに対して電子証明書を使った電子署名を行い、業務上の証拠として残す機能を提供しているものがある。

また、メールファクスについては S/MIME という電子メールのコンテンツを暗号化・電子署名する方式があり、ここで電子証明書が利用される。

文書の処理ではないが、SSL/TLS の暗号化通信機能では、電子証明書を利用したサーバ/クライアントの認証、鍵の交換の機能がある。

3.9.12 基本ソフトウェア(OS) - 入出力ドライバ、シリアル、パラレル、USB、ディスク

一般的に基本ソフトウェア(OS)については、すべてのハードウェアの制御、リソース管理機能などが含まれるが、ここでは特に市販の MFP 製品に共通な機能について特定しておく。

MFP の OS には、複数の組込み製品に汎用的に利用できる、汎用の OS と、そのメーカや機種ごとに限定された専用の OS がある。専用の OS では、OS のソースコードが開示されていなかったり、OS の API も非公開であったりするため、攻撃者への認知度が低い。一方、汎用 OS では Windows、Linux、VxWorks のように広く普及しているため攻撃者への認知度も高いが、標準的な API を利用でき、必要があればソースコードを入手して確認できるというメリットがある。そして共通することだが、どちらの OS でも、高機能化と高性能化に伴って、さまざまな脆弱性をはらむ可能性がある。

MFP の基本ソフトウェア(OS)として、入出力ドライバがある。MFP の外部のインタフェースとして、シリアル、パラレル、USB、ハードディスクの入出力を制御する。

3.9.13 基本ソフトウェア(OS) - ファイルシステム

MFP 内部で、一時的なジョブデータや長期的に保存する共有の文書ファイルを格納する。MFP が格納する設定情報や、利用履歴、監査記録については MFP 内部のファイルシステム上か、データベース上で格納されることがある。

3.9.14 基本ソフトウェア(OS) - ジョブ制御

MFP にはプリント、スキャン、ファクス、コピーなどの複数の要求が指示され、それらが順序良く処理されていかなければならない。それぞれの処理は数分以上かかるものもあり、多くのあとから指示された要求は「ジョブ」という形で MFP 内部のハードディスクやメモリ上に保留される。

ジョブ制御は、受け付け中のジョブ、実行中ジョブ、保留ジョブ、完了ジョブを制御して、なんらかの結果を出すようにジョブを実行する。

3.9.15 基本ソフトウェア(OS) – 時刻

オフィス向きの MFP の場合、運用履歴を記録したログ、認証サーバや暗号化機能、電子証明書などのために、時刻は常にシステム内で同期していなければならない。MFP 上では、リアルタイムクロックと呼ばれる部品が、電源を停止している間も時刻を刻み、電源が投入されたあとも、ほぼ正しい時刻で動作する。ネットワーク上の時刻サーバを利用して時刻を同期させることもある。

3.9.16 基本ソフトウェア(OS) - 暗号、乱数

「暗号」にはハッシュ値を計算する処理や、暗号化を行う処理などが含まれている。「乱数」は一般的に暗号を利用するときに、暗号鍵として予想しにくい値を生成するために重要な役割を果たす。

3.9.17 運用管理 - 設定、構成

MFP の運用管理における「設定、構成」は多くの項目があり、数百項目以上になることもある。個別の設定項目については MFP の機種ごとに依存するため、個別の詳細な設定項目については検討せず、機能ブロック単位での設定に関して検討している。

3.9.18 運用管理 - 停止、開始

MFP には省電力機能があり、自動的に節電モードに入る。また、ファクス搭載機は常時電源を投入するが、ファクスを搭載しない機種では、業務時間外は電源をオフにすることもある。

3.9.19 運用管理 - 稼動記録

MFP のプリントまたはコピーの枚数を利用者ごとに記録し、設定変更やソフトウェアの追加削除など運用管理の履歴を記録する。

3.9.20 運用管理 - 保守、交換、修理

MFP の故障に対応し、ハードウェア部品やソフトウェアの交換をするための機能。ライセンスの管理機能も含まれる。

3.9.21 運用管理 – 自己診断

MFP の故障時に MFP 内部のソフトウェアが MFP 内部のハードウェアやソフトウェアの状態を確認して、故障や不具合箇所を報告する機能。

3.9.22 認証・承認・課金 - 認証、利用者、管理者

MFP が利用者や管理者を認証する機能。保守者も認証する。

3.9.23 認証・承認・課金 - 制限、許可

MFP が特定の利用者グループや全利用者に課す利用制限と許可。

3.9.24 認証・承認・課金 - 係数・課金

特定の MFP でプリントまたはコピー、スキャンなどのサービスが利用された回数や枚数の集計値。MFP 単位で集計され、保守業者が課金する根拠として利用する。

3.9.25 認証・承認・課金 - 監査記録

特に MFP のセキュリティ機能を利用するときに、セキュリティ機能を利用した処理が行われたか、そのセキュリティ処理の結果は成功か失敗か、などの履歴を記録する。定期的な MFP のセキュリティ機能の稼動に関する監査のときに参照、集計される。

3.9.26 通信・ネットワーク - ネットワークサービス提供

MFP が利用者端末や他システムに対してサービスを提供するために、MFP はネットワークからの要求、リクエストが届くのを待機している。MFP は外部の利用者端末や他システムから要求が届くと、この要求に対して何らかの処理を行って応答する。このような、他のシステムに対する要求・処理・応答をネットワークサービスと呼ぶ。

ネットワークサービスは、MFP 内部で動作するサーバによって提供されるため、サーバ機能とも呼ぶ。MFP のサーバ機能には、MFP の機能の共有サービスを提供する SMB サーバや HTTP サーバ、ファイル共有サービスを提供する FTP サーバ、ファクスやスキャンのイメージデータを転送・配信する SMTP サーバなどがある。

また、MFP の管理や保守用にも複数のネットワークサービス機能ある。管理用途では、MFP 内部の稼動状態などを応答したり、状態を変更させたりする SNMP サーバがある。

3.9.27 通信・ネットワーク – リモート管理・制御

管理者が遠隔から MFP の設定を行ったり、構成管理を行ったりするための機能。MFP 上の Web サーバ上で提供されている管理ページまたは保守ページを、管理者端末から開いて利用する。

3.9.28 通信・ネットワーク - 通信制御

IP ネットワーク上の通信制御を指す。「ネットワークサービス」に比較して、通信制御は Ethernet と IPv4/IPv6 の制御の部分を指す。

4. MFP 利用時のデータフロー

MFP を利用するときのデータフローを以下の構成図に従って特定する。データはイメージや文書などのコンテンツデータと、指示や制御などの制御データの二つに分けて整理する。コンテンツデータについては実線で、制御データについては点線で示している。

なお、稼動記録についてはすべての処理で記録が行われる共通の処理であるため、稼動記録の書き込み処理については読み出しのみデータフローを特定した。

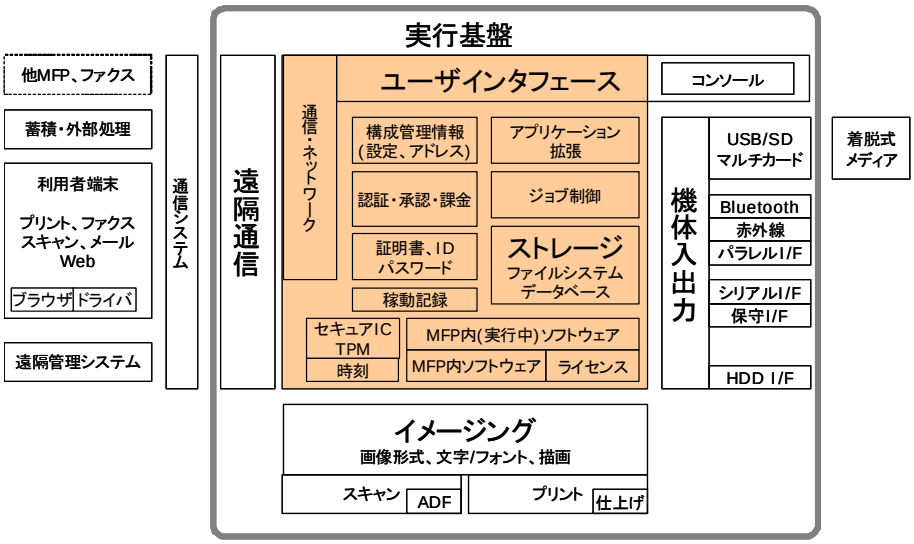

図 4-1 MFP 利用時のデータフローの構成図

4.1　プリント

下の図 4-2はプリントのデータフローである。利用者端末から印刷用のイメージと印刷方法などの指示がMFPに送信される。MFPでは、通信・ネットワークモジュール内のプリント受付機能が接続を受け付ける。接続を受け付けると、保護された通信路の確立を行い、認証処理の後、ジョブを受け付けてファイルシステム内に保存する。

保存されたジョブデータをジョブ制御に通知したあとは、ジョブ制御が他のジョブとの調整を行いながらイメージングユニットにプリントを指示して、印刷物が出力される。

利用者端末を認証して、MFP がその利用者端末用のセッション情報を作成した場合は、ジョブの受け入れが完了した時点で、その利用者端末用のセッション情報を削除する。

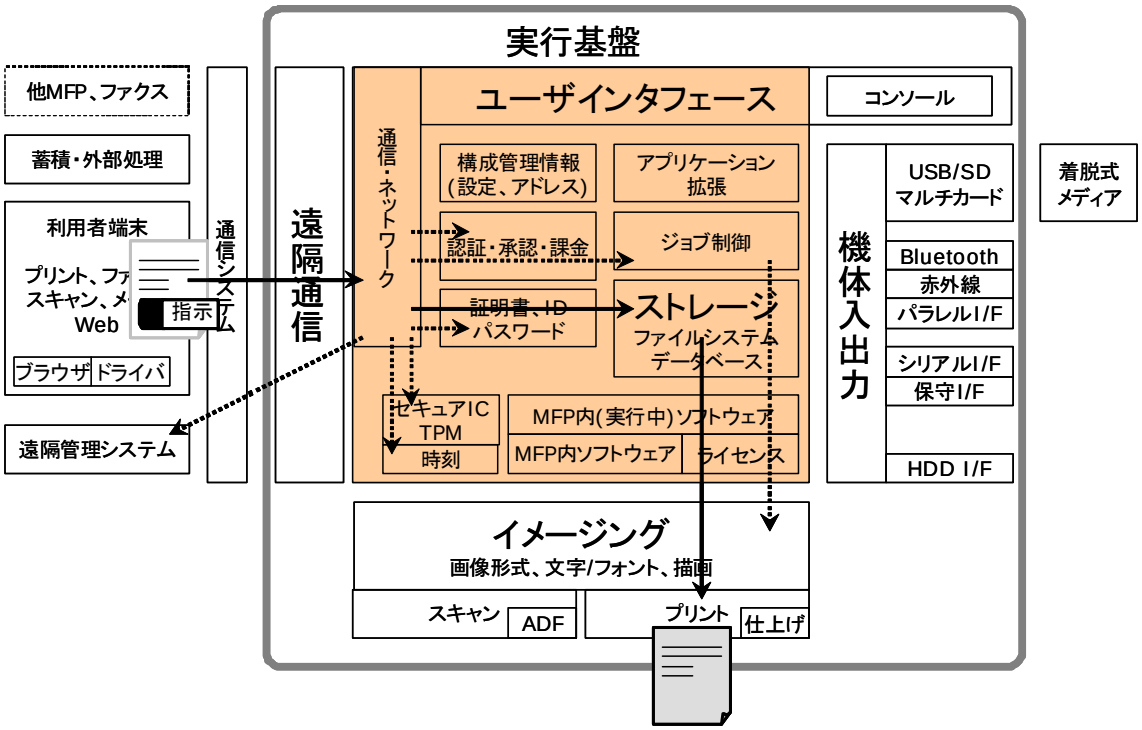

図 4-2 プリントのデータフロー

4.2　負荷分散印刷

下の図 4-3は負荷分散印刷のデータフローである。この図はすでにジョブデータを受信した直後からのデータフローを示している。

ジョブ制御は、ジョブデータに含まれる指示から、構成管理情報を確認して、外部にある MFP のうち、どの MFP に印刷を指示するか、特定する。ジョブ制御は特定された依頼先のアドレスと印刷枚数などの新しい指示データを添えて、アプリケーション拡張にあるブラウザのプリントクライアント機能に印刷指示を行う。

プリントクライアント機能は通信・ネットワーク機能を利用して、他の MFP との間で保護された通信路を確立する。このとき、MFP 内部の証明書やパスワード、セキュア IC、時刻を利用する。保護された通信路を確立すると、プリントクライアントはストレージから指定の枚数でジョブデータを他の MFP に転送する。

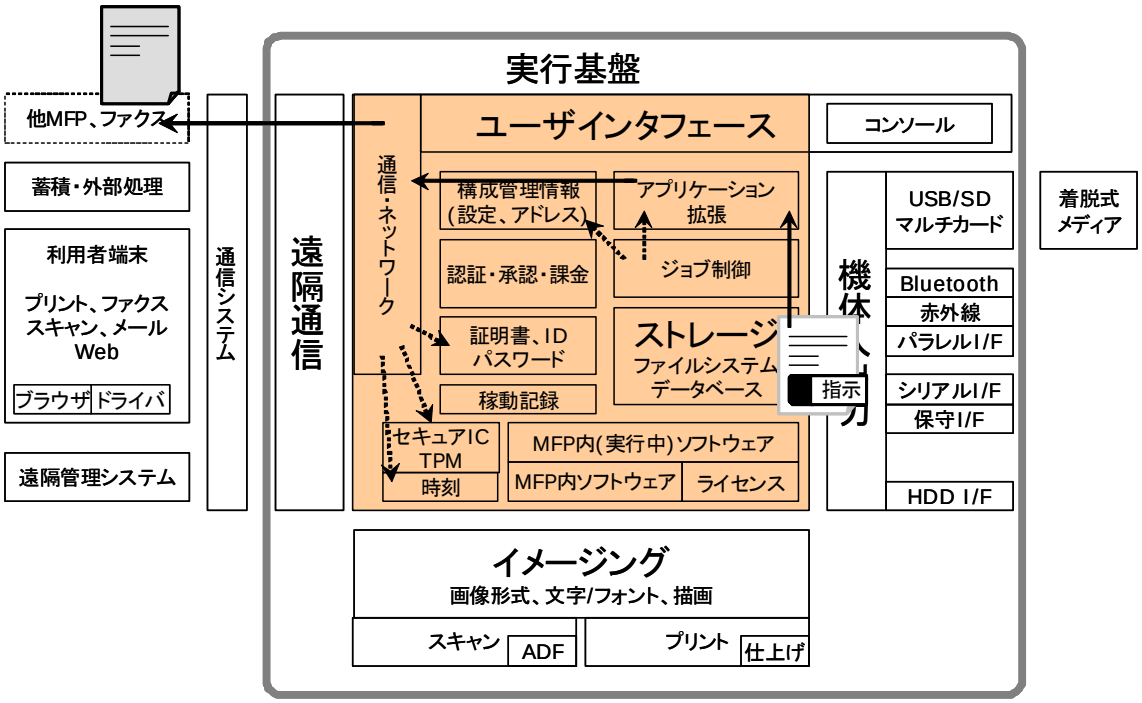

図 4-3 負荷分散印刷のデータフロー

4.3　スキャン to X、ファクス送信

下の図 4-4はスキャンの結果を何かに配信する「スキャン to X」のデータフローを示した図である。ここで言う「X」とは、「何か」という意味の略称である。スキャン to Xには、ファクス送信も含む。

一般利用者は、MFP の前で、MFP に対してコンソールから作業の指示を行う。コンソールからは、スキャンを行って、スキャン結果を何に配信するかを指示する。スキャンの利用に認証が必要な場合は、ユーザインタフェースがコンソールか、MFP のシリアルインタフェースの先に接続した IC カード認証装置や生体認証装置で一般利用者として認証する。

一般利用者はスキャンの方法と宛先を指定する。宛先は MFP 内のアドレス帳から選択する。場合によって、アドレス帳は遠隔通信を経由して、遠隔管理サーバ上の共有のアドレス帳から検索することがある。一般利用者はこのときまでに原稿をスキャン台に置く。

上記で指定された、利用者の識別情報、宛先、スキャン方法はまとめて指示としてジョブ制御に渡される。ジョブ制御はイメージングに制御指示を行い、スキャンユニットでスキャン処理が行われる。スキャン処理の結果、作成されたファイルがイメージングからストレージに渡される。

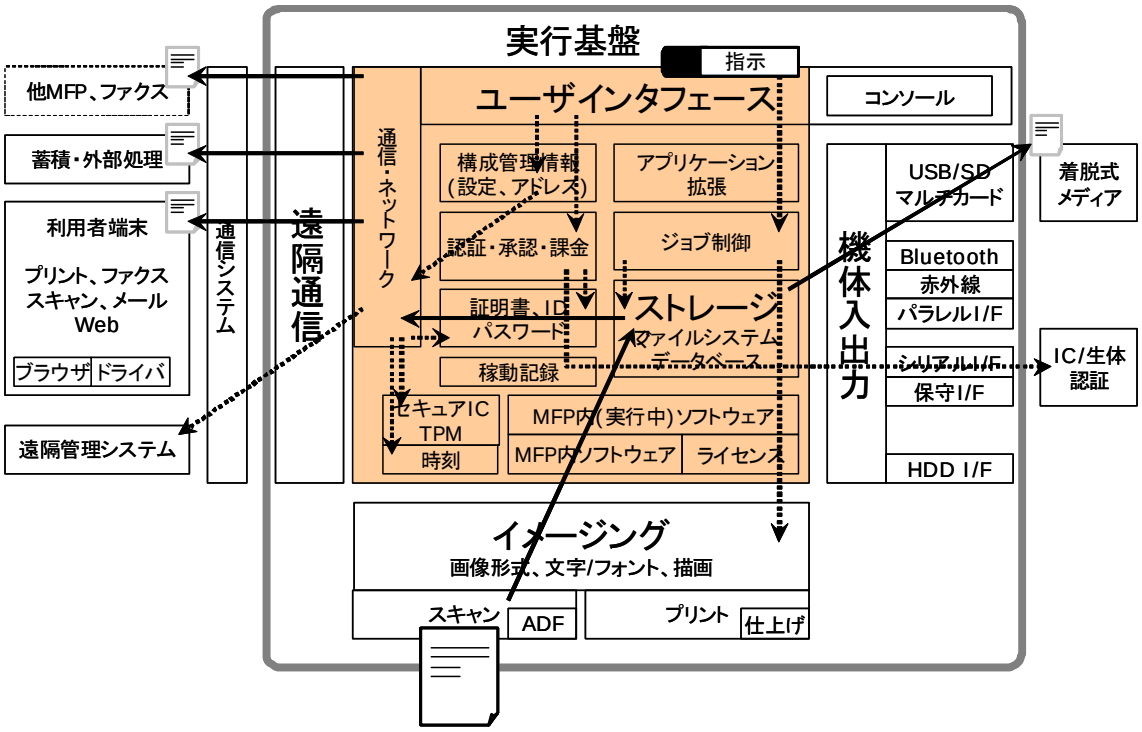

図 4-4 スキャン to X、ファクス送信のデータフロー

ストレージからは、ジョブ制御からの指示に従い、所定の宛先に配信を行う。以下に、この図での配信先を列挙する。

1) 他の MFP、ファクスへの配信: 図の左上
2) 蓄積・外部処理へのサーバ配信: 図の左上から 2 番目
3) 利用者端末へのサーバ配信: 図の左上から 3 番目
4) 着脱式メディアへの配信: 図の右上

上記配信先のうち、着脱式メディア以外については、保護された通信路の確立のために、証明書、ID、パスワードを使った相互認証を行い、セキュア IC と時刻を利用して保護された通信路を確立する。

上記配信先のうち、蓄積・外部処理についてはほとんどの場合、何らかの認証処理が必要になるだろう。その際は一般利用者の指示により指定された認証データを利用するか、遠隔管理システム上の認証サーバとのトークンの交換などを行う。

すべての指定された宛先について配信が完了すると、この処理が完了する。

一般利用者は指示の作業が終了しログアウト手順を実行するか、MFP への操作がなく一定時間が経過すると、MFP は自動的に「証明書、ID、パスワード」に生成されたセッション情報を削除する。

4.4　ファクス受信

下の図 4-5はファクス受信のデータフローを示している。ここではファクスを受信すると、すぐに紙に印刷して排出トレイに排出する手順としている。利用者を識別した上での認証印刷については、プリントの手順で特定している。

図の左上にある「他の MFP、ファクス」で、原稿が読み取られるか、パソコンからファクスイメージが他の MFP、ファクスに送信され、「他の MFP、ファクス」から、「通信・ネットワーク」のファクス受信機能を使ってファクスイメージを受信する。ファクス受信機能には、PSTN ファクス、メールファクス、SIP ファクスがある。メールファクスの場合は、保護された通信路を確立するため、証明書、セキュア IC/TPM、時刻を利用する。SIP ファクスの場合、一般的には保護された通信路を動的に確立はせず、「通信システム」を閉域網や隔離することでセキュリティを確保している。

受信されたファクスイメージはストレージに格納され、受信結果がジョブ制御に渡される。ジョブ制御は構成管理情報にある、ファクスの発番号や着番号によるボックス振り分け条件を確認し、親展ボックスやサーバなどに配信するか、紙に印刷するかなどの、新たな宛先を特定する。

このあとの処理は、「スキャン to X」でスキャンイメージをストレージに格納したあとのデータフローと同じである。

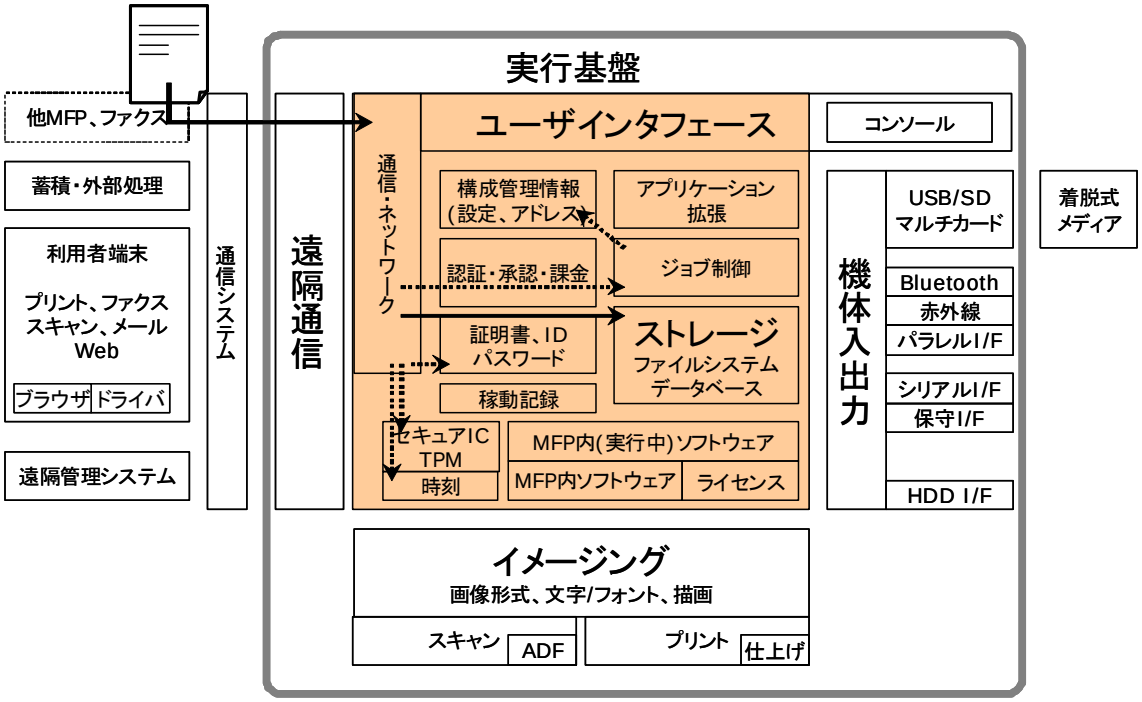

図 4-5 ファクス受信のデータフロー

4.5　コピー

下の図 4-6はコピーのデータフローである。一般利用者はコンソールからコピーの指示を開始する。必要に応じて、ICカードまたは生体認証を使った一般利用者の認証か識別が行われる。また、一般利用者の認証と承認をMFPの外部にある認証サーバと行う場合は、「通信・ネットワーク」を経由して「遠隔管理システム」上の認証サーバに、コピーをしようとする一般利用者の認証を要求する。

一般利用者はコピーの処理条件をコンソールで指定する。事前に設定された設定値のセットや、印刷の負荷分散を指定する場合は、設定構成情報の中に利用者や管理者が設定した情報を参照して利用する。

このときまでに利用者はコピーの原稿をスキャン台や ADF に設置する。

一般利用者によるコピー処理の指示が終わると、指示がジョブ制御に渡され、コピー処理が開始される。ジョブ制御は、イメージングにコピーの指示を行う。原稿がスキャンされ、ストレージに格納される。ストレージに格納されたイメージはプリントに渡されて印刷される。ストレージへの格納は、ハードディスクにファイルを作成する場合と、メモリ(一時メモリ、DRAM)上に格納される場合がある。

一般利用者は指示する作業が終了すると、コンソールでログオフするか、操作がない状態が一定時間経過すると MFP が自動ログオフし、「認証・承認・課金」にあるセッション情報が削除される。

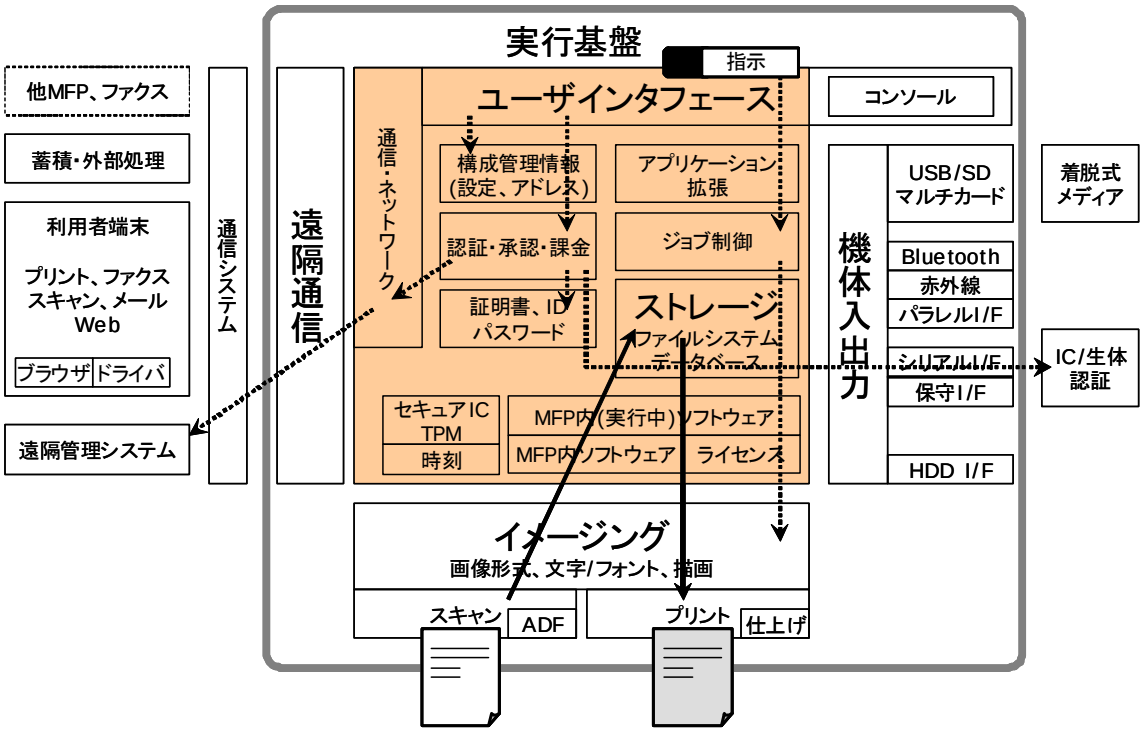

図 4-6 コピーのデータフロー

4.6　構成管理情報の設定、取得(コンソール)

下の図 4-7は、MFP本体の構成管理情報の設定、取得を行うときのデータフローである。MFP本体の構成管理情報には、「証明書、ID、パスワード」や、「セキュアIC/TPM」への操作、「時刻」への変更を含んでいる。また、ここではMFPのコンソールから指示を行う手順を示している。

MFP の管理者はコンソールから構成管理情報の変更指示を行う。そのために管理者の認証手順を行う。ユーザインタフェースは「認証・承認・課金」に指示して、管理者認証処理を行う。必要に応じて IC カードや生体認証を行う。IC カードや生体認証は場合によって「遠隔管理システム」にある認証サーバによる認証が必要である。

管理者認証が済むと、ユーザインタフェースで構成管理情報の設定メニューが表示されるようになり、「構成管理情報」「証明書、ID、パスワード」「セキュアIC/TPM」「時刻」の内容変更または上書き、追加、削除、または内容の取り出しと表示が行われる。セキュア IC/TPM については、秘密鍵などの重要な機密の情報は取り出しができないが、秘密鍵の名前や識別名などについては表示される。

管理者は作業が終了すると、ログアウト手順を実行し、MFP の「証明書、ID、パスワード」に生成されたセッション情報が削除される。

なお、ソフトウェアやライセンスについては保守者が変更するため、管理者は操作しない。

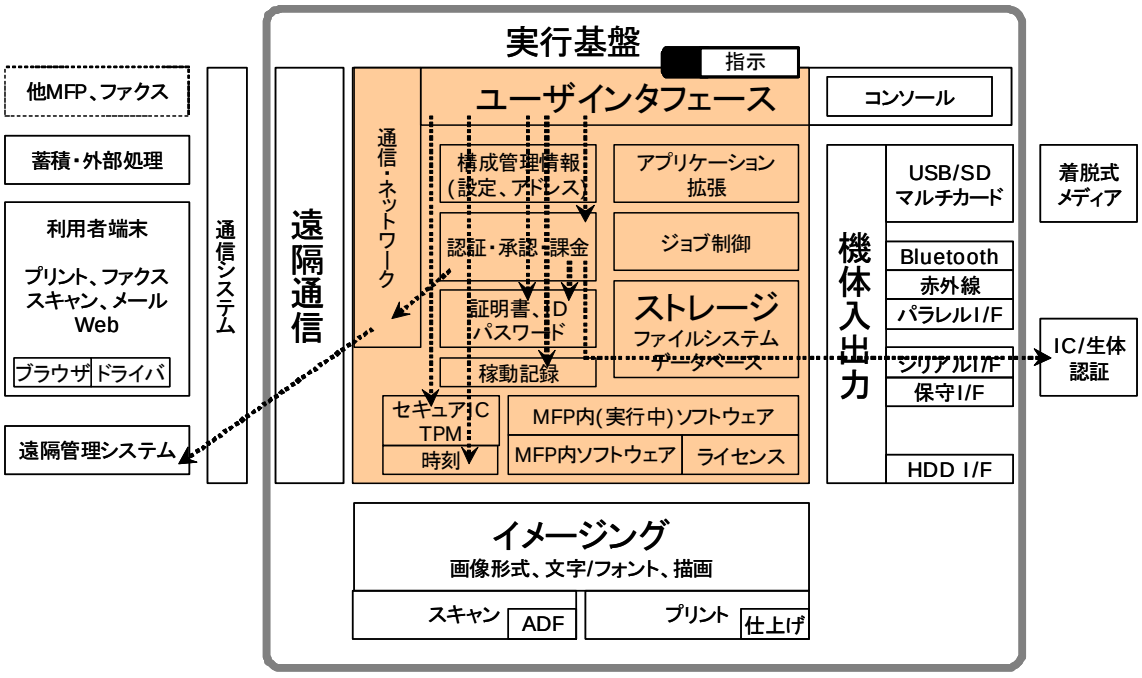

図 4-7 構成管理情報の設定、取得データフロー

4.7　遠隔通信経由での構成管理情報の設定、取得

下の図 4-8は、遠隔通信経由で、MFPの構成管理情報の設定または取得を行うときのデータフローである。

管理者は遠隔管理システムにある、管理者端末から MFP の「通信・ネットワーク」内の Web サーバや SSH サーバなどの管理用サーバに接続し、ログインする。管理者端末と MFP は保護された通信路を確立するため、「証明書、ID、パスワード」と「セキュア IC/TPM」、「時刻」を利用する。また、このあと遠隔から接続要求をしてきた管理者の認証を、MFP から遠隔管理システム上の認証サーバに対して行う。

管理者端末と MFP との間で保護された通信路が確立し、管理者の認証が完了すると、管理者はユーザインタフェースから提示された、設定ページやコマンドラインを操作して、MFP 内部の複数のデータを変化させる。「構成管理情報」については設定値の追加、変更、削除を行う。「証明書、ID、パスワード」についても追加、変更、削除の操作を行う。「セキュア IC/TPM」については秘密鍵とその属性情報の追加または削除を行う。「時刻」については変更のみ行う。共通の操作として、値かデータの読み取りがあるが、「セキュア IC/TPM」については秘密鍵の読み取りはできない。

管理者は作業が終了すると、ログアウト手順を実行し、MFP の「証明書、ID、パスワード」に生成されたセッション情報が削除される。

なお、ソフトウェアやライセンスについては保守者が変更するため、管理者は操作しない。

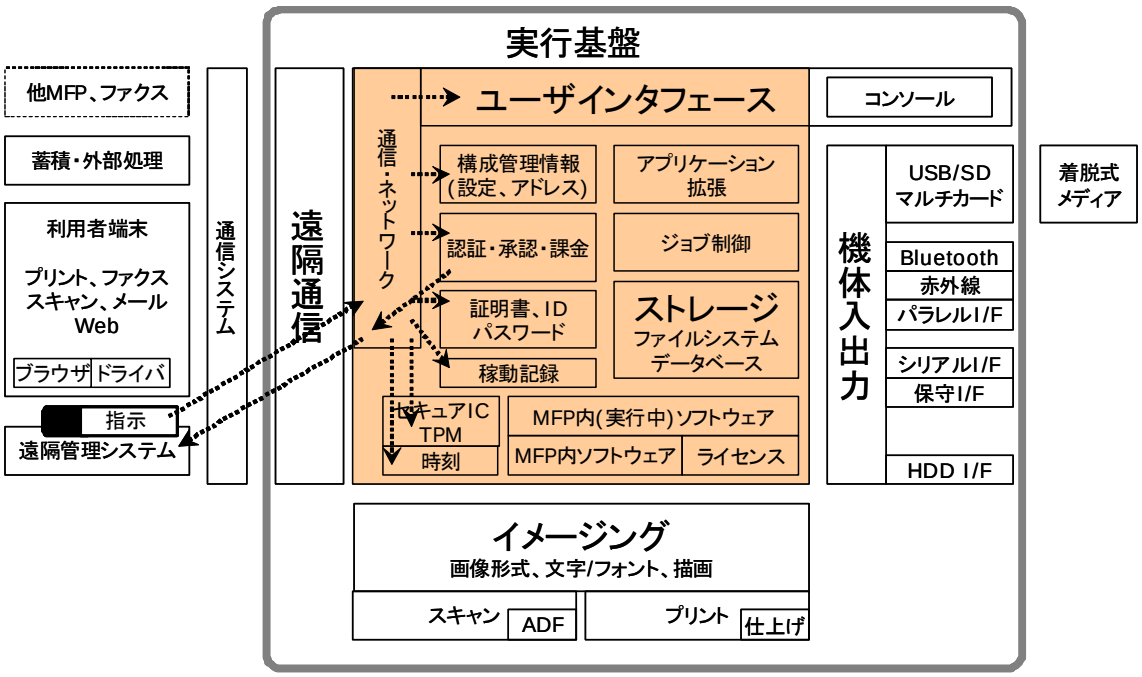

図 4-8 遠隔通信経由での構成管理情報の設定、取得データフロー

4.8　保守作業 部品交換、課金取得、診断

下の図 4-9は保守作業 部品交換、課金取得、診断のデータフローである。

MFP の保守者はコンソールで保守者認証を行う。MFP 外部の認証手順についてはほかのデータフローと共通であるため割愛し、保守者の認証を MFP 本体内で行うデータフローのみを示している。保守者は MFP のコンソールからキーボード入力などで保守者の ID とパスワード文字列を入力し、保守者認証を行う。

保守者認証が完了すると、保守者用のメニューが表示されるので、保守者はコンソールから必要な処理を選択する。場合によっては、保守用インタフェースから保守用パソコンを接続し、保守用パソコン上での簡易メニューかコマンドラインを操作する。保守用インタフェースについては、その存在自体が不明な場合と、存在する場合、認証が不要な場合もある。

点検などの保守作業と部品交換では、通常は診断処理を行う。診断処理では、図中のハードウェアの個別の診断機能の実行と結果取り出し、ファイルやデータの一貫性の検査などがあるが、MFP 内部の診断機能は保守用の取扱説明書に記述され、一般には公開されていないため確認ができていないが、診断可能な対象や項目はメーカや機種によって異なると考えられる。

保守者は作業が終了すると、コンソールでログオフし、「証明書、ID、パスワード」に生成されたセッション情報が削除される。

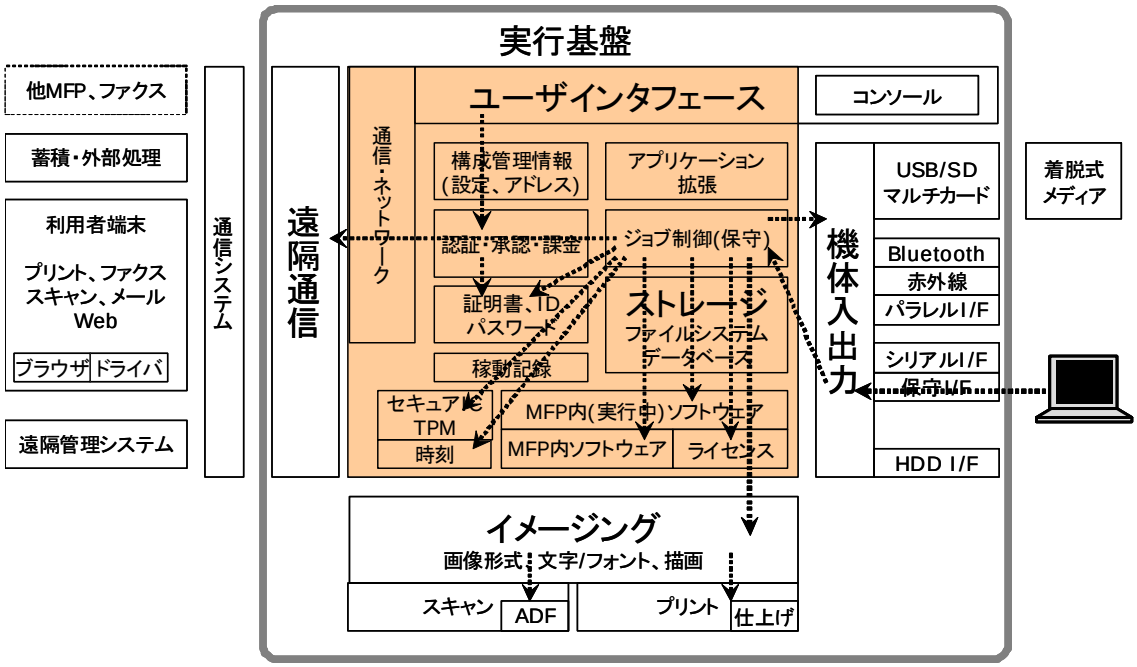

図 4-9 保守作業 部品交換、課金取得、診断のデータフロー

5. MFP の守るべき資産

5.1　MFPを利用する環境での一次資産

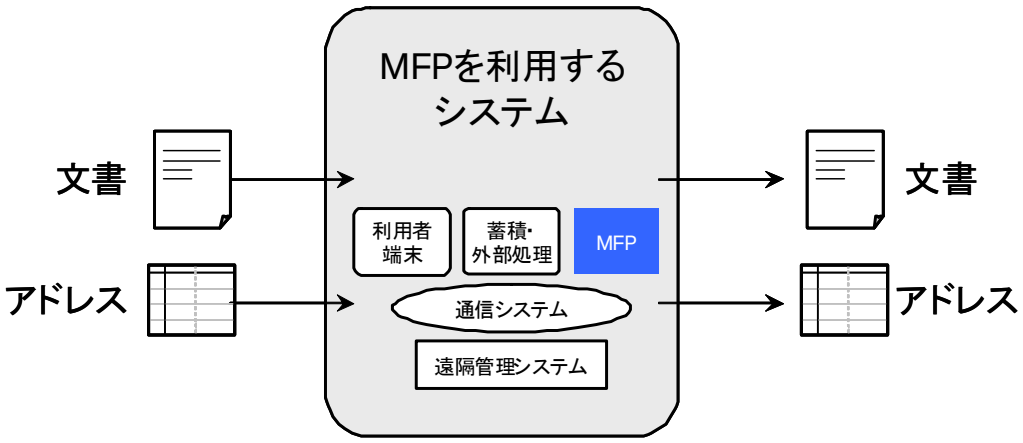

図 5-1 MFP 利用時のデータフロー

利用者から見て、MFPを利用する直接的な目的は、文書の保存と配布である。利用者が文書の保存と配布を行うときに、直接的に守るべき情報資産を「一次資産」として位置づける。上の図 5-1は一次資産である文書とアドレスがMFPを通じて処理が行われる概念を示している。文書は保存や配布したい内容の情報である。アドレスは配布したい宛先をあらわす情報である。

ただし、一次資産は情報の資産であるため、実体を持たない。実体としての情報資産は具体的にはそれぞれの場面で異なる。このように、MFP を情報システムのひとつとして利用するときに、一次資産を守るために必要になる具体的な情報資産を、「二次資産」と位置づける。例えば、文書については紙媒体の場合は原稿や印刷物として具体化する。MFP 上では電子化されたイメージやページの描画内容を記述したデータがジョブデータと呼ばれるファイルやメモリ上のビット列して扱われている。また送付先や配信先のアドレスはジョブデータの中に、制御命令の一部として格納されている。また、認証やセキュリティのための情報も、一次資産を守るために必要となる、二次資産と考えられる。

5.2　MFPを利用するために守るべき対象としての二次資産

下の表 5-1は、MFPの利用環境で関連する二次資産を一覧表にしたものである。大きく 4 つのカテゴリに分類した。

「MFP 本体」は MFP の機器とソフトウェアなどである。USB メモリや SD メモリカードなどの着脱式メディアは、本体ではないが、本体と密接する着脱式メディアであるため MFP 本体に分類した。MFP はこれら機器とソフトウェアがそろうことで、稼動させることができる。

「実行時データ」はコピーやプリントなどの処理が行われる間に交換される情報資産を指す。

「他システム」は、MFP が稼動するために、MFP の外部から認証や管理などのサービス提供する、外部のホストや機器のことを指す。本調査では、MFP 本体の脆弱性が中心となっているため、これら他システムについては、各他システムの

内部の詳細については検討せず、他システムの外部インタフェースにのみ注目して分析を行う。

「稼動結果情報」は、処理後に得られる原稿や印刷物、ファイルや記録を指す。

表 5-1 MFP を利用するために守るべき対象としての二次資産

カテゴリ	二次資産
MFP本体	本体機器 （ハードウェア）
	MFP内ソフトウェア
	使用ライセンス、保守ライセンス
	着脱式メディア
実行時データ	ジョブデータ （スプール,イメージ,宛先,制御）
	管理構成情報
	電子証明書、ID、パスワード、 セッション情報
	正しい時刻

カテゴリ	二次資産
他システム	通信システム （スイッチ、DHCP, DNS, NTP）
	遠隔管理システム （認証、構成管理、監視、保守）
	一般利用者端末
	蓄積・外部処理 （スプーラ、共有フォルダ、メール、 業務システム）
稼動結果情報	原稿、印刷物
	MFP内共有ファイル
	利用履歴、監査記録
	MFP利用課金情報

次の章では、これら二次資産について、さらに詳細に脅威の分析を行うが、以下に、二次資産のそれぞれについて、その概要とセキュリティ上要求される主な点などを参考にまとめておく。

5.3 MFP本体

5.3.1 本体機器(ハードウェア)

MFPの本体機器を指す。「3.8 MFP内部のハードウェア」で説明したように、いくつかのユニットに分割されている。正しい本体機器が装着され、配線されている必要がある。

5.3.2 MFP内ソフトウェア

MFPを動作させるためのソフトウェア。「3.9 MFP内部のソフトウェア」で説明したように、複数のモジュールやアプリケーションに分かれて搭載されている。

ソフトウェアは追加や更新が比較的容易に行えるが、MFP 内には正しいソフトウェアが必要である。不正ソフトウェアは排除される必要がある。

5.3.3 使用ライセンス、保守ライセンス

利用者が MFP を利用する間、搭載しているソフトウェアの利用権や、保守サービスの利用権が使用ライセンスや保守ライセンスとしてメーカか販売業者、保守業者から発行され、それぞれの MFP 内部に登録される。

ライセンスにはさまざまな契約条件があるが、一般的にライセンスは期間が限定されており、契約期間が過ぎるとライセンスが無効になり、そのライセンスに該当する機能も停止する、という前提で分析を行う。逆に、契約していないライセンスが登録されると、予定していなかった機能やサービスが動作してしまうこともある。

5.3.4 着脱式メディア

USB フラッシュメモリや SD メモリカードなどのように、簡単に挿抜して移動できるメディアのことを指す。MFP 本体ではないが、直接本体に装着してよいハードウェアであるため、本体に分類した。

着脱式メディアには、利用者が文書を交換するために利用するものと、保守者が MFP の管理情報やソフトウェアの構成などを行うためのものがある。利用者向けの着脱式メディアのスロットと、保守者向けの着脱式メディアのスロットは別になっており、用途も異なるが、脅威と脆弱性の一覧では、異なる扱いが必要な場合はそのつど記述する。

5.4 実行時データ

5.4.1 ジョブデータ(スプール、イメージ、宛先、制御)

ジョブデータとは、プリント、ファクス、コピー、配信などのイメージデータと制御情報を記録したものである。

イメージデータには、原稿や印刷物の表示領域の画像を再現するための、デジタル化されたイメージや描画命令などが含まれる。

制御情報には、転送先のアドレスまたは宛先とその転送手順、印刷物の排出先や仕上がりの条件などがある。仕上がり条件には、印刷物での画像の配置方法などの画像処理方法、印刷部数や出力トレイなどが含まれる。仕上がり条件に従った処理は、フィニッシャと呼ばれる装置で処理される。

また、制御情報には認証情報を含むことがある。例えば、利用者を認証してプリントする場合で、認証サーバを利用せず MFP 内に設定された利用者名だけを利用した簡易な認証プリントの場合は、ジョブデータ内に利用者端末で入力された利用者名やユーザ ID が書き込まれ、MFP 内の利用者ごとのスプールにジョブデータが保存されるものもある。

5.4.2 管理構成情報

MFP を所定の条件で動作させるために MFP に設定、登録する情報、または MFP 内に保存された設定情報。

MFP が所定のサービスを提供し、必要なセキュリティを確保するために認証などセキュリティ機能を動作させ、他システムと連携するために必要なアドレスやパス名、番号、呼び名の文字列など。

管理構成情報には、MFP が所定の機能を停止させるための情報や、特定の利用者には特定の機能を利用させない、などの制限のための情報も含む。

5.4.3 電子証明書、ID、パスワード、セッション情報

認証を求められたときに応答する電子情報。電子証明書は公開鍵証明書と、秘

密鍵の二つの情報に分かれている。このうち秘密鍵は、秘密鍵を情報として取り出しできないようなセキュア IC や TPM などの格納装置に保存し、認証時にはセキュア IC に計算処理を行わせて照合する。ID とパスワードは認証処理時に照合処理が必要なため MFP 内部のストレージか、MFP 起動時に参照できる不揮発メモリ内に格納しておく。

セッション情報は、サービスを利用する利用者や他システムの利用セッションごとに許可を与えるためのトークンのようなもので、Web ブラウザのクッキー情報や、URL に含まれるセッション ID、HTTP POST リクエストの要求データ内に含まれるセッション ID なども該当する。

5.4.4 正しい時刻

ファクスで送受信の履歴を記録するときに必要になる。稼動の履歴情報を記録する際にも、記録としてそのときの時刻もいっしょに記録する。稼動の履歴情報にある時刻は、他システムや他の MFP の記録と照らし合わせて確認するときのために、同じ正しい時刻に合わせておく必要がある。

また、暗号通信や署名・検証を行うための基本となる情報である。自己署名証明書の時刻としても重要である。

認証・認可・課金の機能では、認証された時刻や認可を継続できる時間幅などを管理するため、認証サーバやシングルサインオン機能を提供するサーバと MFP の間で、同期した正しい時刻が必要である。

ソフトウェアのライセンスについては、ライセンスの期間が特定されている場合は、正しい時刻との比較が必要である。

5.5 他システム

5.5.1 通信システム(スイッチ、DHCP、DNS、NTP)

MFP 本体と遠隔通信をする他システムを接続するための通信機器と、ネットワークの基盤的な情報を提供するサーバ。

通信機器には、Ethernet スイッチやルータ、あるいは無線 LAN のアクセスポイントなどと、これら機器の配線が含まれる。

ネットワークの基盤的な情報を提供するサーバには、DHCP サーバ、DNS サーバ、NTP サーバがある。DHCP サーバは、IP アドレスの自動割当とルータの IP アドレス、DNS の IP アドレスの配布を行う。DNS サーバはホスト名から IP アドレスを検索する要求やその逆の検索などに応答する。NTP サーバは複数の MFP やシステム内のホストの間で時刻を同期させるため、現在の正確な時刻を応答する。

5.5.2 遠隔管理システム(認証、構成管理、監視、保守)

遠隔管理システムには、認証サーバと、構成管理サーバ、監視サーバ、保守端末などが含まれる。

認証サーバは利用者の ID とパスワード、または証明書情報などを集中して保持し、MFP を含む他のホストからの利用者を認証する要求に応答する。構成管理サーバは管理者が複数の MFP を一括して設定できるなどの機能がある。監視サーバは 1 台以上の MFP の稼動状態を定期的に取り出して、異常があると管理者や別のシステムに通報をする機能がある。

保守端末は MFP の保守が必要なときに MFP の内部の診断を行ったり、ソフト

ウェアやライセンスの追加と削除を行う。こうした保守作業については端末ではなく保守サーバが定期的に処理を行う場合もある。

5.5.3 一般利用者端末

プリント、ファクス送信、スキャン開始、MFP 内に一時的また長期に格納されたファイルの取得など、MFP の一般利用者向けのサービスを利用するための端末。一般利用者端末がファクス受信するときは MFP 内からのファイル取り出しを行う形になる。一般利用者端末からコピーを実行することはない。

これら MFP の一般利用者向けのサービスは、運用者または保守者が利用することはない。試験用に利用する場合は一般利用者として実行するものとする。また、一般利用者端末から MFP 内部の設定やアドレス帳などの構成管理情報を変更することはないものとする。

一般利用者端末上では一般的に、特定の機種の MFP に対応したドライバソフトウェアを追加インストールする。ドライバソフトウェアには、MFP にプリントやスキャンイメージ取出しを指示するときに必要なパス名や、ID・パスワードなどを設定することがある。メールファクスを利用する場合は、その利用者のメールアドレスやクライアント証明書を指定する場合もある。

5.5.4 蓄積・外部処理(スプール、共有フォルダ、メール、業務システム)

MFP の外部にあって、文書の蓄積や配信を行う。一般的には直接人が操作しないサーバとして動作している。MFP を利用するための情報システムの一部であり、ジョブのスプールサーバ、共有フォルダやメールサーバ、業務システム用の Web サーバなどがある。スプールサーバは、MFP へのプリントジョブを一時保留しておくサーバで、利用者に対する認証機能や、MFP に対するジョブデータの分配機能、負荷分散処理機能がある。共有フォルダは、電子ファイルを格納するディスクをネットワーク上で複数の利用者が共有するためのサービス。メールサーバは、メールファクスやメールでの配信に利用される、メールの送信受付サーバ(SMTP)、メールの転送サーバ(SMTP)、メールボックス内への電子メールメッセージを提供するメールボックスサーバ(POS3, IMAP4)からなる。

メールの転送サーバとメールボックスサーバは、MFP を利用する組織の外にある場合がある。また、ファクスの宛先に当たる MFP も他組織である場合もある。これらの他組織の間では、機密情報保護契約などが結ばれて、それぞれが交換した機密を保護することを前提とする。ただし、MFP の脆弱性については、異なるメーカや機種の MFP を利用したとしても、どちらの組織にも同じように脆弱性が発生するものとみなす。

5.6 稼動結果情報

5.6.1 原稿、印刷物

コピーまたはスキャンで MFP に読み取りさせる紙が原稿。コピー、プリント、ファクスで MFP から出力される紙が印刷物。文書の内容を含む。

5.6.2 MFP内共有ファイル

MFP 内部で共有されている電子ファイルで、文書のイメージを含む。一部は宛

先や、PDF やジョブデータのように追加の制御情報を含むものもある。共有ファイルは MFP の外部の一般利用者端末が閲覧、更新することができる。

5.6.3 利用履歴、監査記録

ある MFP 上で、どの利用者がいつ何をしたか、どこから何のリクエストがあり、どのような結果になったか、という情報。サーバやホストのアドレスや、処理を行ったときの認証 ID を含むことがある。また、場合によって一部 MFP では入力間違いがあったパスワード文字列が ID として記録されている場合がある。

利用履歴と監査記録は MFP 内部に記録する場合と、MFP の外部に記録する機能がある。

これらの記録は、定期的に利用者か運用者が内容を集計または抽出して検査・検討し、その後の運用に役立てる役目がある。

5.6.4 MFP利用課金情報

保守者が収集する情報で、MFP でプリントやコピーをした枚数や回数の情報など。保守者はこの情報をもとに利用者に対して保守料金や利用料金を請求し、利用者は保守者に支払いを行う。

6. 脆弱性の分類

6.1 CWE共通の脆弱性タイプと、本資料で扱う分類

下の図 6-1は、情報関連製品の脆弱性情報を収集する非営利団体のMITRE[9]が、これまでによく知られた脆弱性を体系的に分類した系統図である。本調査では、MFPの脆弱性の網羅性を保つため、既存の脆弱性の分類から、MFP製品にも同様の脆弱性が存在するであろうと仮定し、分類ごとの脆弱性の有無を検討する。そのために利用する脆弱性の分類として、下の図 6-1の赤枠の分類を利用することとした。CWEにある脆弱性タイプには、「不適切な入力確認」や「不適切な認証」、「リソース不足」などの典型的な脆弱性のタイプが列挙されており、MFP製品にもあてはまると考えられるタイプが多い。

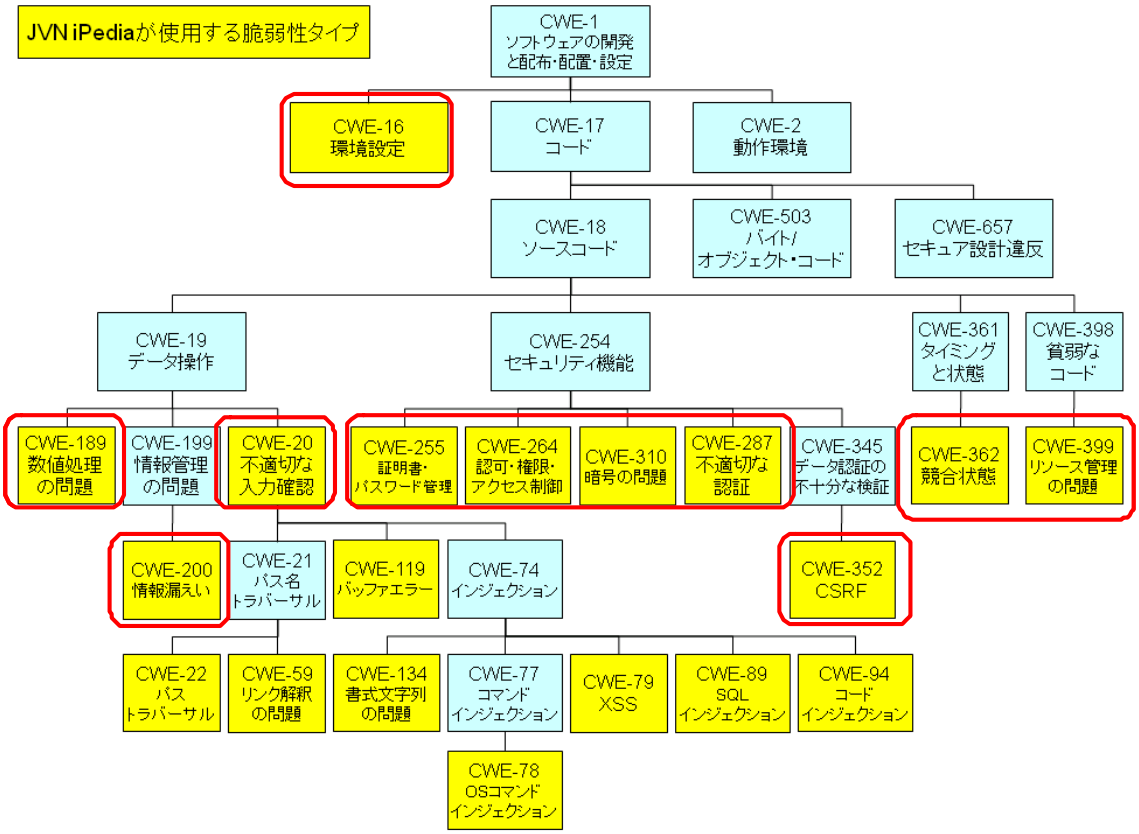

図 6-1 CWE共通の脆弱性タイプと、本資料で扱う分類[10]

本調査では、複数の MFP 製品の機種に適用する関係で、特定の MFP 機器の実装を特定した調査は行わない。そのため「CWE-20 不適切な入力確認」以下の分類は MFP 製品の個別の実装に依存するため、「CWE-20 不適切な入力確認」にまとめた。本調査では、CWE の脆弱性分類の階層のうち、5 段目の分類レベルを中心に利用する形となっている。

[9] MITRE Corporation：米国政府向けの技術支援や研究開発を行う非営利組織。
http://www.mitre.org/

[10] CWE共通の脆弱性タイプ - http://www.ipa.go.jp/security/vuln/CWE.html#cwes

「その他」「CWE 以外」「情報不足」「設計上の問題」については本調査では分類できないものが多いため「その他」にまとめた。また、CWE は主にソフトウェア製品の脆弱性を分類しているが、本調査では「操作間違い」と「表示上の不具合」についても脆弱性を抽出するため、CWE 脆弱性タイプの「その他」に含める形で分類した。

表 6-1 本資料で利用する脆弱性タイプ

MFP で利用する脆弱性タイプ		CWE 識別子
W01	環境設定	CWE-16
W02	不適切な入力確認	CWE-20
W03	数値処理の問題	CWE-189
W04	情報漏えい	CWE-200
W05	証明書・パスワード管理	CWE-255
W06	認可・権限・アクセス制御	CWE-264
W07	不適切な認証	CWE-287
W08	暗号の問題	CWE-310
W09	クロスサイト・リクエスト・フォージェリ（CSRF）	CWE-352
W10	競合状態	CWE-362
W11	リソース管理の問題	CWE-399
W12	その他(操作間違い、表示不具合、停止・起動、故障)	CWE-Other

7. 脅威から想定される脆弱性

本章では、MFP の利用環境における脅威の一覧から、それぞれの脅威において原因となると考えられる脆弱性を列挙する。ここでは、情報が何かの媒体の上に存在した状態での具体的な脅威を検討するため、二次資産についてのみ脅威を列挙する。

7.1 脅威の抽出

本章では、脅威を網羅的に特定するため、二次資産のそれぞれについて求められる情報セキュリティの要求事項を、7 つのタイプごとにあてはめて検討する。7 つのタイプの要求事項を下の図 7-1に示す。

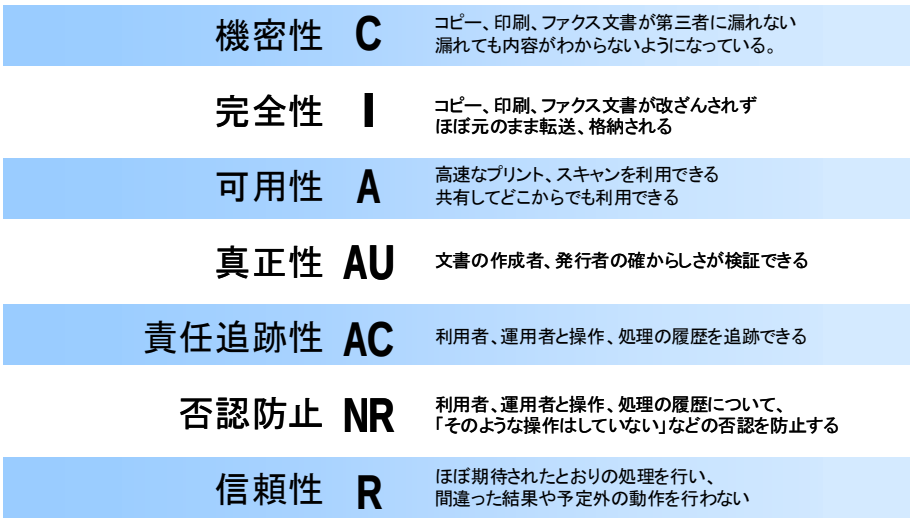

図 7-1 情報セキュリティの要求事項 – 7 つのタイプ

「5 MFPの守るべき資産」で特定した 16 種類の二次資産のそれぞれについて、セキュリティの要求事項を破る想定を行い、脅威を列挙する。列挙した脅威は、次の「7.2 本体機器（ハードウェア)」から、表の「T. この二次資産に対する脅威」の列に記録する。さらにこれらの脅威それぞれについて、考えられる脆弱性を列挙する。脆弱性の列挙を行う場合は、「6 脆弱性の分類」で整理した脆弱性の各タイプが原因となることを想定しながら列挙した。

脅威の原因となりそうな脆弱性を列挙するときには、現段階でそれなりの攻撃手法や、利用間違いなどの実現性が想定できることを確認するため、攻撃手法の例を最低 1 例は特定するようにした。また、被害の例について、それぞれの表の下に二次資産ごとの被害例を記載している。

被害の影響度の目安として、二次資産ごとに共通脆弱性評価システム「CVSS 2.0」の基本評価基準の一部、「AV:攻撃元区分」、「AC:攻撃条件の複雑さ」、「Au:攻撃前の認証要否」について評価値を記入している。これら評価値は、その二次資産で列挙したさまざまな攻撃手法から、影響度の範囲を示す形になっている。CVSS 2.0 についての詳細はIPA「共通脆弱性評価システムCVSS概説」[11]を参照い

[11] IPA「共通脆弱性評価システムCVSS概説」 - http://www.ipa.go.jp/security/vuln/CVSS.html

ただきたい。なお、本調査では考えられる脆弱性を網羅することが目的であり、各攻撃手法と前提条件は詳細に特定していない。そのため影響度についてはあくまで参考としてごらんいただきたい。

7.2 本体機器（ハードウェア)

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
1. 機密性	・MFP 本体内部の端子や配線の途中に直接接続されて盗聴される。または、MFP 本体内部の機器に電気的な影響を与えられ、盗聴される	・MFP 本体内部の基盤上のバス、デバッグ端子、モジュールのバス端子、機器の接続端子などに電気的に接続し、バス上または端子上の通信データを盗聴する	・MFP 本体内部の機器や端子に直接電気的に接続できる脆弱性 ・MFP 本体内部のユニット間インタフェースが標準インタフェースとなっており接続方式や通信方式を容易に予測できる脆弱性 ・MFP 本体のユニット間インタフェース上の通信データが保護されていない脆弱性
		・攻撃者は電源スイッチ ON または OFF 操作直後に、特定のキーボード操作を行うか、シリアルポートからブレーク信号を送るなどの操作により、認証操作なしで MFP を特権状態で動作させ、MFP の保護機能をオフにする	・機能モジュールが電気的な影響で停止または誤動作する脆弱性 ・MFP に電源投入後の起動中または停止指示後の停止処理中に特定のキー操作またはハードウェア割り込みを発生させると特権状態で動作してしまう脆弱性
		・攻撃者は保守者になりすまして MFP の実行基盤上の DRAM を含むボードを取り出し、DRAM を冷却しながら DRAM 内部のデータを読み取り、DRAM 上に残されていた暗号鍵が攻撃者に漏洩する	・電源切断後、実行基盤上の DRAM を冷却しておくと、しばらく DRAM の内容を読み取れる脆弱性 ・DRAM 上の暗号鍵が保護されていない脆弱性
		・攻撃者が実行基盤上の不揮発メモリ(FlashROM など)か HDD を取り出して MFP 内ソフトウェアのコピーを容易に入手する	・第三者が実行基盤にハードウェア的にアクセスしやすい環境にある、人為的脆弱性 ・実行基盤上のストレージに格納されたソフトウェアが保護されていない脆弱性
2. 完全性	・MFP 本体機器の一部または全部の機器、配線が入れ替えられる	・MFP 本体内の HDD を入れ替えられ、HDD 内の保護されていない機密文書や、保護されていないアドレス帳、保護されていない証明書、ID、パスワードを、攻撃者が入手する[本体機器の入れ替え]	・第三者が実行基盤にハードウェア的にアクセスしやすい環境にある、人為的脆弱性 ・ストレージに格納されているデータが保護されていない脆弱性
		・攻撃者によって、印刷の排紙口、ADF の内部に追加のスキャナを装着させられ、機密の原稿と印刷結果のイメージを、追加スキャナまたはフラッシュメモリの交換や無線経由で攻撃者が入手する[本体機器の入れ替え]	・MFP 本体内部や本体に任意の追加の機器を容易に取り出し、装着される脆弱性

		・攻撃者が実行基盤上の不揮発メモリ(EEPROM, NVRAM など)を交換して MFP 用の設定、構成管理情報を書き換える[機器の入れ替え]	
3. 可用性	・本体機器の一部または全部が盗難または破壊され、MFP を利用できない ・電源、通信の配線が抜かれるか撤去されて MFP を利用できない ・電源の電圧が頻繁に大きく変動するために MFP が起動せず、動作しても途中で停止する	・MFP 本体内部の暗号化用ハードウェアモジュールや実行用一時メモリの盗難、破壊により MFP が利用できなくなる ・MFP 本体用、スキャナ用の電源ケーブルが盗難され、MFP を利用できなくなる ・MFP 本体内部の一部機器に電源系統や信号切り替え系統などに、直接接続して電気的な負荷を与えるか、電磁波によって電気的な負荷を与えて、MFP の動作を停止させる	・第三者が実行基盤にハードウェア的にアクセスしやすい環境にある、人為的脆弱性 ・本体内部の機器や端子に直接、第三者がアクセスでき、MFP 本体内部の一部機器や部品を持ち出せる脆弱性 ・第三者が実行基盤にハードウェア的にアクセスしやすい環境にある、人為的脆弱性 ・機能モジュールが電気的な影響で停止または誤動作する脆弱性 ・ハードウェアモジュールが外界からの電磁波を受けて誤動作する脆弱性
4. 真正性	・本体に装着されている機器が適切な正しい機器であるかどうか確認できないため、機器の追加、取り外しがあってもわからない	・MFP 本体内に偽の HDD ユニットを装着し、機密文書のジョブデータやファイルそのものを記録させ、HDD を交換することで攻撃者が機密文書とアドレスの一部を入手する	・本体内または本体に直接接続されている HDD やプリントエンジン、仕上げ機器などが、正当な機器であるかどうか確認できない脆弱性
5. 責任追跡性	・本体機器の一部または全部の追加、取り外しがあっても、その詳細や原因を確認できない	・攻撃者によって MFP 本体内の HDD を入れ替えられたが、いつ、どの利用者が入れ替えたかわからないため、対策を検討できない	・本体内または本体に直接接続されている HDD やプリントエンジン、仕上げ機器などを追加・取り外ししても記録が残らない脆弱性
6. 否認防止	・本体機器の一部または全部の追加、取り外しが、保守者によって行われたことがあるのに、特定の保守者が行ったということを立証できない	・攻撃者によって MFP 本体内の HDD を入れ替えられたが、MFP が記録する保守の監査履歴には、なりすまされた偽の保守者 ID が注入されたため、対策を検討できない	・履歴に他の利用者の名前、ID・パスワード、セッション情報を再利用して、なりすましができる脆弱性(検証できない脆弱性) ・履歴の記録を行うとき、任意の時刻や、任意の利用者名を記録できてしまう脆弱性

7. 信頼性	・本体機器内の一部機器や配線の間違い、部品の欠落、不足などにより、適切な処理が行われない	・MFP 本体内部の配線が間違っており、暗号化モジュールがバイパスされ、HDD への暗号化処理が行われずにデータが記録され、MFP 廃棄時に残存していた機密の文書が漏洩する	・本体機器内の配線または装着箇所の間違い ・「基本動作」や「セキュリティモード」などの所定の用途を実現するときに、MFP 本体内部の機器と配線の構成(リソース容量や処理能力、機能の有無など)が正しいかどうか検証できないか、検証していない脆弱性
		・一時メモリの不足があると、処理の一部だけが不完全な出力や配信が行われ、不具合があったこと自体がわからない	
		・MFP 内部で電子証明書の生成を行う際に、MFP 内部にセキュア IC/TPM が存在しない場合、電子証明書の秘密鍵が保護されていないハードディスク上のファイルに保存され、MFP 内部に侵入した攻撃者に秘密鍵が漏洩する	

7.2.1 想定される被害の例

1) 継続的に、保護されているはずの機密の文書が漏洩するか、改ざんされる
2) 継続的に、アドレス帳が漏洩するか、改ざんされる
3) MFP 使用中か廃棄後に証明書、ID、パスワードが漏洩する
4) MFP をほぼ全面的に利用できなくなる(一般利用者、管理者、保守者)

7.2.2 およそのCVSS 2.0 基本評価基準(一部)の影響度

1) AV:攻撃元区分　　ローカル～ネットワーク
2) AC:攻撃条件の複雑さ　高～中
3) Au:攻撃前の認証要否　複数～不要

7.3 MFP 内ソフトウェア

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
1. 機密性	・MFP 内部の実行前の格納されたソフトウェアが漏洩する ・MFP 内部の実行中のソフトウェアの情報が漏洩する	・MFP 内部に格納されたソフトウェアを遠隔の管理システムから追加、更新するときに、途中の通信システム上で盗聴され、ソフトウェアが漏洩する	・MFP と遠隔の管理システムとの間の通信が保護されていないか、保護が不完全である脆弱性
		・MFP 内部のデバッグインタフェースに接続し、認証なしでデバッグインタフェースを制御し、MFP 内部のファイルシステムに指示してソフトウェアを取り出す	・デバッグインタフェースは JTAG や GDB など標準的なコマンド体系が実装されており容易に推測される脆弱性 ・MFP 内部のソフトウェアを取り出すインタフェースが稼動し、認証なしで利用できるようになっている脆弱性
		・MFP 内部で動作するソフトウェアのいずれかの脆弱性を利用して任意のコードを注入し、(特権モードを取得して、)MFP 内部のファイルシステムに指示してソフトウェアを取り出す	・MFP 内部で任意のコードが実行させられる脆弱性 ・MFP 内部の特権モード(管理者モードまたは MFP 内部の権限不要状態)での制御を奪取される脆弱性
		・攻撃者が、本来残存していないはずの MFP のデバッガインタフェースに接続することで、MFP 内部の実行中のソフトウェアのシンボル名、実行時アドレス、機械語命令を入手し、その MFP 用に侵入して攻撃を実行するためのソフトウェアを開発し、販売する	・MFP のデバッグインタフェースが動作したまま残っている脆弱性(MFP 内部の機械語レベルでのソフトウェアの実行状態が容易に奪取または制御される脆弱性)
		・攻撃者が実行基盤上の不揮発メモリ(FlashROM など)にアクセスして MFP 内ソフトウェアのコピーを容易に入手し、このソフトウェアの内容と動作を容易に解析して、脆弱性を特定し、攻撃コードを開発し、販売する	・外部に取り出された MFP 内ソフトウェアを容易に解析またはリバースエンジニアリングできる脆弱性
		・あるサードパーティが MFP 用の SDK を利用して開発した拡張アプリケーションで、MFP 内部のアドレス帳の内容を認証なしですべて応答する機能が悪用され、アドレス帳の内容が漏洩する	・SDK を利用してサードパーティが開発した拡張アプリケーションが MFP 内部の特権モードで動作するとき、特定の機密のデータを認証なしで公開してしまう脆弱性
2. 完全性	・MFP 内ソフトウェアの一部または全部が不正なソフトウェアに入替、追加させられるか、一部ソフトウェアが停止または削除され、適切な処理ができない(実行前、実行中)	・MFP 内部で、利用されないはずの拡張アプリ実行サービスが動作しており、攻撃者が任意の命令を実行させて、機密の文書を入手する	・MFP 内部で動作させていないはずのサービス、または待ち受けていないはずのポートが開いている脆弱性(設定が間違っている場合、攻撃者がソフトウェアを追加して構成情報の制御をバイパスして動作させていた場合、SDK を利用した拡張アプリケーションが間違えてポートを開いている場合)

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
		・MFP 内部の一部ソフトウェアが、利用者または認証がない利用者でも書き換え可能な場所に配置されるため、攻撃者が任意のコードを追加して、MFP の処理の途中で機密の文書を入手する	・MFP 内部のソフトウェアが、保守者以外でも書き換え可能な場所に配置されている脆弱性
		・MFP 内部のソフトウェアを遠隔の管理システムから追加、更新するときに、途中の通信システム上で通信データが改ざんされ、不正なソフトウェアが注入される	・MFP と遠隔の管理システムとの間の通信が保護されていないか、保護が不完全である脆弱性
		・MFP 内部または外部のデバッグインタフェース、ソフトウェア交換インタフェースに接続し、認証なしでインタフェースを制御し、MFP 内部のファイルシステムやソフトウェア更新機能に指示して不正なソフトウェアを追加、更新する	・MFP内部のソフトウェアを追加、書き換えるインタフェースが稼動し、認証なしで利用できるようになっている脆弱性
		・攻撃者が LPR の入力脆弱性を利用して不正コードを注入することにより、MFP 内部の監査記録機能が停止させられ、操作履歴が記録されないまま稼動を続けたため攻撃者のその後の操作内容がわからないまま攻撃の被害にあった	・入力されたデータにより MFP 内部で任意のコードが実行させられる脆弱性 ・MFP 内部の特権モードでの制御を奪取される脆弱性
		・攻撃者がMFPの入力脆弱性を利用して、MFPが受け付ける特定のサービスポートでの認証機能だけがバイパスされるように実行中のソフトウェアにフックを挿入し、以後攻撃者が認証なしで MFP を攻撃し、他システムへのなりすましのアクセスが行われ、他システムの業務データが漏洩する	・MFP 内部で実行される特定のソフトウェア機能がバイパスまたは停止させられたまま実行が継続してしまう脆弱性
		・攻撃者が MFP の入力脆弱性を利用して、MFP 内部の乱数生成機能を改ざんし、常に同じ乱数を返すようにする。この乱数生成機能を使った暗号化処理で処理された SSL/TLS の暗号通信を、攻撃者が解読し、他システムのパスワードや機密の文書が漏洩する	
3. 可	・MFP 内ソフトウェアの一部または全部が削除または破壊されるか、ソフトウェアの脆弱性を悪用して動作を停止させられ、MFP を利用できない(実行	・MFP 内部のソフトウェアを遠隔の管理システムから更新するときに、途中の通信システム上で通信データが改ざんされ、破壊されたソフトウェアが注入される	・MFP と遠隔の管理システムとの間の通信が保護されていないか、保護が不完全である脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
用性	前、実行中)	・MFP 内部、外部のデバッグインタフェース、ソフトウェア更新インタフェースに接続し、認証なしでインタフェースを制御し、MFP 内部のファイルシステムかソフトウェア更新機能に指示して、ソフトウェアを削除するか、破壊されたソフトウェアで書き換えする	・MFP 内部のソフトウェアを削除、書き換えするインタフェースが稼動し、認証なしで利用できるようになっている脆弱性
		・MFP 内部で動作するソフトウェアのいずれかの脆弱性を利用して任意のコードを注入し、(特権モードを取得して、)MFP 内部のファイルシステムに指示してソフトウェアを削除、書き換えする	・MFP 内部で任意のコードが実行させられる脆弱性 ・MFP 内部の特権モードでの制御を奪取される脆弱性
		・SDK を利用した一部の拡張アプリケーションがメモリを大量に消費し、MFP 本体のサーバ機能が停止してしまう	・SDK を利用した一部の拡張アプリケーションが CPU またはメモリなどのリソースを大量消費し、MFP 本体の機能か、拡張アプリケーションの機能を停止させる脆弱性
4. 真正性	・MFP 内ソフトウェアまたはダウンロードやメモリで導入しようとするソフトウェアが適切なソフトウェアかどうか確認できないため、ソフトウェアのすり替えがあってもわからない	・保守者が間違って古いバージョンのソフトウェアを導入してしまい、一部の機能が使えなくなってしまった	・MFP に追加、更新されるソフトウェアが正当なものであるか検証できない脆弱性
		・その MFP 用に拡張アプリケーションとしてソフトウェアを配布することが認められていないサードパーティの開発者が、MFP の内部にインストールできる拡張アプリケーションを作成し、特定の MFP にインストールする	
5. 責任追跡性	・MFP 内ソフトウェアが改ざんをされていたとしても、その原因を特定できない	・保守者が間違って古いバージョンのソフトウェアを導入して、一部の機能が使えなくなってしまったが、どの保守者がどのインタフェースを経由して行ったのか特定できず、損害賠償ができない	・保守者権限を複数の人が共有しているため実行者を特定できない脆弱性 ・保守操作で利用者の認証が行われていない脆弱性 ・保守操作の履歴が記録されていない脆弱性 ・保守操作の履歴に時刻、利用者名、操作名の必須情報がない脆弱性
6. 否認防止	・MFP 内ソフトウェアの一部または全部の入替えが、保守者によって行われたことがあるのに、特定の保守者が行ったということを立証できない	・特定の保守者が間違って古いバージョンのソフトウェアを導入したという記録があったが、その保守者は否認しており立証する証拠がない	・他の利用者の名前、ID・パスワード、セッション情報を再利用して、なりすましができる脆弱性(検証できない脆弱性) ・履歴、監査情報の記録を行うとき、任意の時刻や、任意の利用者名を記録できてしまう脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
7. 信頼性	・MFP 内部に追加または更新するソフトウェアが正しい場所に配置されなかったり、間違ったコードや不正なコードを混入させられたり、ソフトウェアの一部が欠落することでMFPを正しく動作させられない ・MFP 内部のソフトウェアの脆弱性が発見されて、実際に悪用される	・保守者が実施する、遠隔からのソフトウェアの更新手順の途中で、通信終了を示すパケットを注入するか、手順を飛び越えてソフトウェア更新完了メッセージを注入することでソフトウェアを不完全な形で書き込みさせる	・追加、更新対象のソフトウェアが正しく書き込まれたか検証できない脆弱性 ・ソフトウェアが正しく書き込まれたことを検証する処理をバイパスまたは中断できる脆弱性
		・攻撃者が、特定の MFP に対して侵入試験、ファジング試験を行い、脆弱性を発見し、MFP 上の脆弱性を攻撃し、MFP 上で任意のコードが実行される	・MFP 内部のソフトウェア試験の計画、実施が充分に行われていない脆弱性(自社開発または外部から導入した OS やライブラリ、ミドルウェアを含む)
		・SDK を利用した複数の拡張アプリケーションを導入した MFP で、複数の長大なジョブデータが投入されると、メモリの取得で競合が発生し、ジョブデータが失われる	・SDK を利用した複数の拡張アプリケーションの競合による脆弱性
		・善意の第三者が脆弱性を発見してメーカに通報してきたが、回答をせず脆弱性への対応もしなかったため、通報者が脆弱性を公開し、悪意の攻撃者が攻撃用ソフトウェアを開発販売し、大規模に被害が発生し、損害賠償を請求される	・MFP の脆弱性が発見されたあとの体制と対応方法の計画がない人為的脆弱性
		・攻撃者は、MD5 ハッシュ関数がコリジョンを起こしやすい脆弱性を利用して、ファクスメールの S/MIME 署名されたメッセージを改ざんし、正しく電子署名したかのように見せて着信させる	・暗号とハッシュ関数が必要な暗号強度に満たない脆弱性
		・MFP が SSL/TLS 接続をしようとすると、RSA 暗号の 512bit 長の鍵処理にした対応していなかったため、SSL サーバ証明書の 1024bit RSA 鍵を持つサーバに SSL/TLS で保護された接続ができない	
		・MFP が SSL 3.0 と TLS 1.0 の両方に対応していない	

7.3.1 想定される被害の例

1) MFP 内部の保護されていないソフトウェアが漏洩し、契約がない別の利用者に再利用される
2) 継続的に、保護されているはずの機密の文書が漏洩するか、改ざんされる
3) 継続的に、保護されたアドレス帳が漏洩する
4) MFP 使用中か廃棄後に証明書、ID、パスワードが漏洩する
5) MFP をほぼ全面的に利用できなくなる(一般利用者、管理者、保守者)
6) MFP が別の攻撃を実行するホストとして悪用される(任意のコードが実行させられる)

7.3.2 およそのCVSS 2.0 基本評価基準(一部)の影響度

1) AV:攻撃元区分　　ローカル～ネットワーク
2) AC:攻撃条件の複雑さ　高～中
3) Au:攻撃前の認証要否　複数～不要

7.4 使用ライセンス、保守ライセンス

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
1. 機密性	・特定ユーザ環境での MFP の使用ライセンス許可情報が漏洩、暴露し、第三者が利用した使用ライセンス費用、保守ライセンス費用を負担させられる	・MFP のコンソール上で、その MFP に登録されているライセンス情報を表示させ、ライセンスコード文字列などのメモをとり、別の MFP にライセンス情報として入力して利用する	・MFP のライセンスとして MFP に入力または登録するべき文字列が、MFP 上で表示できる脆弱性
		・MFP 上の公開フォルダに、ネットワークか USB 経由でアクセスし、ライセンスとなる電子ファイルを取り出し、別の MFP に入力、登録して利用する	・MFPのライセンスとなる電子ファイルがMFP上で誤って公開されている脆弱性
		・MFP 内のハードディスクに登録されているライセンス情報を、直接 HDD をスキャンして取り出す。暗号化されている場合は暗号鍵をスキャンして取り出す	・MFP のストレージ上のライセンス情報が暗号化やハッシュ化などで保護されていない脆弱性 ・ライセンス情報を暗号化するときの暗号鍵が充分に保護されていない脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
2. 完全性	・使用ライセンスの一部または全部が入れ替えられ、契約利用者の MFP 内のソフトウェアが動作しないか、未契約利用者の MFP が動作してしまう	・中古などの MFP に、別の利用者のライセンスが投入されて販売され、未契約の利用者が MFP を利用する	・別の MFP のライセンス情報がそのまま利用できる脆弱性 ・保守者以外の利用者か、未認証の利用者が MFP にライセンス情報を投入できる脆弱性 ・ライセンス情報に有効期間がない脆弱性 ・ライセンス情報内の機種名やシリアル番号、ソフトウェア名など、特定の固有情報が検証されていない脆弱性
3. 可用性	・時刻を変えるなどして使用ライセンスを無効な状態にされ、MFP を利用できなくなる	・すでに正しいライセンス情報を入力した稼動中の MFP で、不適切なライセンス情報を入力しなおしたため MFP が動作しなくなる（操作間違いまたは攻撃）	・MFP 本体内に無効なライセンスデータを投入され、MFP が利用できなくなる脆弱性
		・すでに正しいライセンス情報を入手した稼動中の MFP で、MFP の時刻を 1 年早く入力してしまったため、契約期間の 1 年前に MFP が動作しなくなる（操作間違いまたは攻撃）	
4. 真正性	・使用ライセンスが正しいライセンスかどうかわからないため、偽造された使用ライセンスにより、未契約利用者が MFP を利用できる	・他の MFP で利用されていたライセンス情報や、それに似せたライセンス情報を、再販売業者や中古業者などの攻撃者が MFP に投入して、MFP を利用する	・発行されたライセンス情報が、特定機種だけではなくほかの機種でも利用できてしまう脆弱性 ・発行されたライセンス情報が、MFP 内部で充分に検証されておらず、第三者が作成したライセンス情報でも MFP が動作してしまう脆弱性
		・ライセンス情報が数桁の数字であるため、順番に加算して試すことで登録可能なライセンス情報を特定し、悪用される	・MFP のライセンスとして MFP に入力すべき文字列が、容易に予想できる数字や、順序のある文字である脆弱性
5. 責任追跡性	・使用ライセンスが無効にされるか偽造されていたとしても、その原因を特定できない	・ライセンス情報を入れ替えても記録が残らないため、他社のライセンス情報を投入した MFP を中古として販売される	・ライセンス入れ替え操作の履歴が記録されていない脆弱性 ・ライセンス入れ替え操作の履歴ログが充分な情報を含んでいない脆弱性［日付、利用者名、アクセス経路、操作内容、結果］
6. 否	・使用ライセンス/保守ライセンスの削除または入替えが保守者によって行われたのに、特定の保守者が行ったということを立証できない	・組織内部の攻撃者は、ライセンス情報を入れ替えると記録が残るので、記録上の利用者名を書き換えるか、任意の別の利用者名が操作したような記録を追加して、MFP が動作	・ライセンス入れ替え操作の記録に利用者名が記録されていたが、その利用者名は利用者から任意の文字列を投入できる脆弱性［ログが任意の利用者名を受け付ける脆弱性］

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
認証防止		しなくなるライセンスを投入し、サービス停止攻撃を行う	・ライセンス入れ替え操作の記録に利用者名が記録されていたが、その記録は第三者が改ざん可能な脆弱性［ログが改ざんされることがある脆弱性］
7. 信頼性	・特定のライセンスデータや特定の環境条件により、無効なライセンスデータが有効と判定されるか、有効なライセンスデータを有効と判定できない	・ライセンス情報の検証機能に不具合を起こさせるようなライセンス情報を作成して MFP に投入し、契約がない利用者が MFP を利用するか、攻撃者が任意のコードが実行する	・ライセンス情報に特定の値が含まれていると、正しいライセンス情報を「不正」と判定してしまう脆弱性 ・ライセンス情報に予想外の値が含まれていると、ライセンス検証機能が中断し、ライセンス検証機能がバイパスされてしまう脆弱性

7.4.1 想定される被害の例

1) ライセンス情報が漏洩し、別の契約がない利用者の MFP によってライセンスを不正使用される
2) ライセンス情報を改ざんされ、別の契約がない利用者の MFP によってライセンスを不正使用される
3) 契約がある利用者の MFP が、ほぼ全面的に利用できなくなる(一般利用者、管理者、保守者)

7.4.2 およそのCVSS 2.0 基本評価基準(一部)の影響度

1) AV:攻撃元区分　　ローカル～ネットワーク
2) AC:攻撃条件の複雑さ　高～中
3) Au:攻撃前の認証要否　複数～不要

7.5 着脱式メディア(利用者用、管理者/保守者用)

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
1. 機	・着脱式メディア上に保護されずに記録された情報が、着脱式メディアの盗難により漏洩する	・着脱式メディアのスロットに挿入されたままのメディアを、攻撃者が抜き出して入手する。または異なる利用者が間違って回収して、機密の文書が漏洩する	・MFP のすぐ前に立ったり座ったりしていても、着脱式メディアの抜き忘れが、視覚的聴覚的にわかりにくい脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
密性	・着脱式メディアのスロット内で、スロットとメディアの間の接点で転送される情報が盗聴される	・MFP 内の、パスワードを含む管理構成情報をバックアップした SD カードが、抜き忘れのため管理者以外の者に抜き取られ、コピーされて機密の文書が漏洩する	・着脱式メディアに記録された機密の文書または管理構成情報などの二次資産が暗号化などで保護されてない脆弱性
		・着脱式メディア上の電子ファイルは暗号化されていたが、暗号鍵がそのメディアに共通の文字列だったため攻撃者に機密の文書が漏洩してしまう	・着脱式メディア上の電子ファイルは暗号化されていたが、暗号鍵が予想しやすい、またはそのメディアに共通の文字列である脆弱性
		・攻撃者は MFP に挿入したまま抜き忘れられた着脱式メディアを入手し、着脱式メディアの暗号化機能で使われているデフォルトの共通パスワードを使って、着脱式メディア内に残っていた機密の文書を入手する	
		・スロットとメディアの間の接点またはスロット側の装置内にプローブが装着され、付属の盗聴装置から送信され、攻撃者に機密の文書か、パスワードを含む管理構成情報が漏洩する	・着脱式メディアと、メディアスロットの間の転送データが暗号化されていないか、保護が不完全である脆弱性
2. 完全性	・着脱式メディア内の保護されていない情報が改ざんされる	・着脱式メディアのスロットにメディアが挿入されたあと、抜き忘れられたメディアを抜き取って、メディア内にあった、ほかにコピーがないオリジナルの機密の文書を書き換えられる	・着脱式メディアのスロットではメディアの挿抜に制限がない脆弱性 ・着脱式メディア上で文書データを保護していない時弱製
		・着脱式メディアのスロットにメディアを挿入されたあと、抜き忘れられたメディアを抜き取って、メディア内にあった、他の MFP に投入するための構成情報を書き換えられ、他の MFP 20 台に投入してしまう	・着脱式メディアのスロットではメディアの挿抜に制限がない脆弱性 ・着脱式メディア上で文書データを保護していない時弱製
		・着脱式メディア上の電子ファイルは暗号化されていたが、暗号鍵がそのメディアに共通の文字列だったため攻撃者に構成情報を書き換えられてしまった	・着脱式メディア上の電子ファイルは暗号化されていたが、暗号鍵が予想しやすい、またはそのメディアに共通の文字列である脆弱性
		・スロットとメディアの間の接点またはスロット側の装置内に介入装置が挿入され、機密の文書または管理構成情報が書き換えられる	・スロットとメディアの間の接点またはスロット側の装置内にプローブが装着され、付属の盗聴装置から文書が送信され、攻撃者に機密の文書が漏洩する
3. 可用性	・着脱式メディアが盗まれるか破壊されるか、読み書きの利用を遮断され、その着脱式メディアを利用できなくなる	・オリジナルのデータが保存してあった着脱式メディアを抜き忘れたあと、攻撃者か異なる人に回収されたため、オリジナルのデータを利用できなくなる	・MFP のすぐ前に立ったり座ったりしていても、着脱式メディアの抜き忘れが、視覚的聴覚的にわかりにくい脆弱性
		・着脱式メディアのスロットを破壊して着脱式メディアを利用できなくする	・着脱式メディアスロットは小型で、物理的攻撃に弱い脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
4. 真正性	・ある特定の着脱式メディアが、その組織の管理者によって承認されたメディアかどうか、確認できない	・攻撃者は MFP の不具合を発生させるための SD カードを何枚も用意して順番に試し、MFP 内部に侵入し、機密の文書が漏洩する	・着脱式メディアに識別機能、認証機能がない脆弱性
5. 責任追跡性	・ある特定の着脱式メディアへの読み書きの履歴をさかのぼって利用者を特定できない	・MFP 内部から着脱式メディアに機密の文書が大量に転送され、攻撃者に漏洩したと考えられるが、どの利用者が実行したのか特定できない	・着脱式メディアの操作について利用履歴が記録されない脆弱性
6. 否認防止	・ある特定の着脱式メディアに関する読み書きの履歴に残された利用者の ID および時刻の記録について、立証できる根拠がない	・SD カードから大量の写真の印刷処理が実行されていたが、記録にある利用者 ID では、誰が実行したのか確認できなかった	・操作の記録に利用者名が記録されていたが、その利用者名は利用者から任意の文字列を投入できる脆弱性［ログが任意の利用者名を受け付ける脆弱性］
		・あるSDカードから不正な構成情報が投入されたが、どのカードから投入されたのか特定できなかった	・操作の記録に利用者名が記録されていたが、その記録は第三者が改ざん可能な脆弱性［ログが改ざんされることがある脆弱性］
7. 信頼性	・MFP に装着した着脱式メディアについて、メディア内のディレクトリや電子ファイルの内容が一部読み込めないか、ファイル名をジョブの名前として表示できなくなる	・SD カードに 2GB を超える長さのファイルを保存しし、MFP で読み込もうとしたところ、それ以外のファイルが読み込めない	・着脱式メディアで特定の大きさ以上のファイルがあると、処理が途中で異常終了する脆弱性
		・SDカードのファイル名に特定の言語のUnicode文字を使うと、ファイル名として表示されず、操作メニューが初期状態に戻る	・着脱式メディア上のファイル名に予想外の文字を書き込んでおくと、任意のコードが実行される脆弱性

7.5.1 想定される被害の例

1) 保護されていない構成管理情報、証明書、ID、パスワードが漏洩、改ざんされる
2) 継続的に、保護されているはずの機密の文書が漏洩するか、改ざんされる
3) 保護されているはずのアドレス帳が継続的に漏洩する
4) MFP 使用中か廃棄後に証明書、ID、パスワードが漏洩する
5) MFP をほぼ全面的に利用できなくなる(一般利用者、管理者、保守者)
6) MFP が別の攻撃を実行するホストとして悪用される(任意のコードが実行させられる)

7.5.2 およそのCVSS 2.0 基本評価基準(一部)の影響度

1) AV:攻撃元区分　　ローカル
2) AC:攻撃条件の複雑さ　高～低
3) Au:攻撃前の認証要否　不要

7.6 ジョブデータ(イメージ,宛先,制御)

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
1. 機密性	・MFP 本体内、他システム間で交換されるジョブデータが漏洩し、文書とアドレスが漏洩する	・攻撃者が一般利用者用の USB メモリポートに、別の USB ハブを介入させ、MFP に入力するジョブデータを盗聴する	・MFP 内部のユニット間のインタフェース上で送受信されるジョブデータか通信路が、保護されていないか保護が不完全である脆弱性
		・以下の経路のいずれかで MFP が交換するジョブデータを盗聴する: MFP 内部のバスや端子、MFP と外部 USB 機器の間、MFP と外部の Bluetooth または赤外線通信機器の間、MFP と IP/AppleTalk/IPX で通信する機器の間 または以下のジョブ伝送手順の経路: IP, TCP, RAW9100, LPR, HTTP, FTP, SMB, IPP, SOAP, WebDAV, SMTP, POP3, IMAP4, SSL/TLS, IPsec, Ethernet, 無線 LAN, USB, Bluetooth, 赤外線/IrDA, AppleTalk, IPX, パラレルインタフェース	・MFP と利用者端末、他システム、遠隔管理システムとの間で送受信されるジョブデータか通信路が、保護されていないか保護が不完全である脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
		・メールファクスのメールヘッダは S/MIME で暗号化されないため、攻撃者は SMTP、POP3、IMAP4 の保護されていない通信路で盗聴して宛先と発信者アドレスを収集する	
		・以下の機器内のいずれかで、ジョブデータが権限のない者に入手される: MFP 内部の HDD、利用者端末内、ジョブデータをスプールする蓄積・外部処理サーバ、proxy サーバ、着脱式メディア	・他システム上で扱われるジョブデータが保護されていないか、保護が不完全である脆弱性
		・攻撃者は一般利用者端末内に侵入し、残存していた保護されていないジョブデータを入手し、機密の文書が漏洩する	
		・攻撃者は保守交換されて一部が故障した MFP 用に利用されていたハードディスクを盗み、ハードディスク上に残っている保護されていないジョブデータから、機密の文書を入手する	・MFP 上で扱われるジョブデータが保護されていないか、保護が不完全である脆弱性
		・攻撃者は MFP に多数のリクエストを送信して、MFP を過負荷にし、MFP がジョブデータの削除または上書き消去できないようにする。その後攻撃者は別の脆弱性を利用して MFP 内部のスプールファイルをとりだし、機密の文書が漏洩する	・ジョブデータの処理終了時にジョブデータが削除または上書き消去されない脆弱性
2. 完全性	・MFP 本体内、他システム間で交換されるジョブデータが改ざんされ、文書の内容または排出先、保存先ボックス名、宛先のアドレスなどが改ざんされる	・以下の保護されていない通信経路のいずれかで MFP が交換するジョブデータが改ざんされる: MFP 内部のバスや端子、MFP と外部 USB 機器の間、MFP と外部の Bluetooth または赤外線通信機器の間、MFP と IP/AppleTalk/IPX で通信する機器の間	・MFP 内部のユニット間のインタフェース上で送受信されるジョブデータが保護されていないか、保護が不完全である脆弱性 ・MFP と機体入出力機器との間で送受信されるジョブデータが保護されていないか、保護が不完全である脆弱性
		・攻撃者は MFP と他システムの間の通信路に介入し、ジョブデータを改ざんして攻撃者宛のアドレスを挿入し、ジョブデータのコピーを攻撃者にも送信し、機密の文書が漏洩する 介入対象は以下のジョブ伝送手順のいずれかの経路上: : IP, TCP, RAW9100, LPR, HTTP, FTP, SMB, IPP, SOAP, WebDAV, SMTP, POP3, IMAP4, SSL/TLS, IPsec, Ethernet, 無線 LAN, USB, Bluetooth, 赤外線/IrDA, AppleTalk, IPX, パラレルインタフェース	・MFP と遠隔通信機器との間で送受信されるジョブデータが保護されていないか、保護が不完全である脆弱性
		・以下の機器内のいずれかで、ジョブデータが権限のない	・他システム上で扱われるジョブデータが保護されていないか、保

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
		者にジョブデータが改ざんされる: MFP 内部の HDD、利用者端末内、ジョブデータをスプールする蓄積・外部処理サーバ、proxy サーバ	護が不完全である脆弱性
3. 可用性	・ジョブデータの伝送と処理ができなくなり、MFP のコピー/プリント/ファクス/配信機能が利用できなくなる	・MFP の処理で予想外の値を含むジョブデータを連続的に作成して MFP に与え、停止や誤動作を起こすジョブデータを調べ(ファジング)、繰り返し停止させる 以下のジョブ伝送手順の処理機能を誤動作させるか過負荷を与えて動作を停止させる: IP, TCP, RAW9100, LPR, HTTP, FTP, SMB, IPP, SOAP, WebDAV, SMTP, POP3, IMAP4, SSL/TLS, IPsec, Ethernet, 無線 LAN, USB, Bluetooth, 赤外線/IrDA, AppleTalk, IPX, パラレルインタフェース, ITU-T T.30	・予想外のジョブデータを受信するか処理すると、誤動作してしまう脆弱性
		・攻撃者は、特定の MFP と他システム(利用者端末、蓄積・外部処理、遠隔管理)との間の特定のセッションに対し、各伝送手順で終了または中断を意味するメッセージ(TCP FIN など)、またはセッションを喪失させる鍵交換不良メッセージなどを注入し、そのセッションを異常終了させる	・MFP と他システムとの間の通信路が保護されていない脆弱性
		・MFP のジョブ伝送以外の、VLAN 認証機能、通信機能、遠隔管理用機能、外部認証機能をを誤動作させるか過負荷にし、ジョブ伝送を停止させる: 802.1x, EAP, DHCP, DNS, NTP, SNMP, SSH, TELNET, LDAP, Kerberos, X.509, OCSP	・受付可能な処理要求量を見積もって、処理要求量を制限できない脆弱性
		・MFP と他システムとの間の通信路を破壊、切断するか、電磁的に干渉してジョブデータの転送を妨害する	・MFP を利用するために使われる通信システムが、攻撃者から物理的に破壊または変更可能な状態にある脆弱性
		・MFP と機体入出力機器の間の通信路で配線を切断するか、電磁的・光的に干渉してジョブデータの転送を妨害する	・MFP と機体入出力機器の間で攻撃者が物理的、電磁的、光的に干渉できる配置構成になっている脆弱性
		・MFP 内部バスかユニット間の配線を切断するか、電磁的に干渉してジョブデータの転送を妨害する	・MFP 本体内部に容易に電気的に接続できるか、電磁的に干渉できるようになっている脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
4. 真正性	・ある処理要求について、ジョブデータを投入しようとする利用者または他システム名が正しいかどうか確認または検証ができない	・認証のないジョブデータ伝送手順(LPR, RAW9100 など)を使って MFP にジョブデータを投入し、利用者ではない者が MFP で印刷する	・ジョブデータの伝送手順自体に認証機能そのものがない脆弱性
		・MFP 上で動作するLPR,RAW9100 サーバでは、ジョブデータを受け入れる接続を確立するときに認証手順がないため、攻撃者は何度でも認証なしで攻撃し、脆弱性を発見することができ、次の攻撃を成功させることができる	
		・他の MFP の IP アドレスを発アドレスに持つ偽装マシンを使って、他の MFP になりすました攻撃者が、特定の MFP にジョブデータを投入し、印刷を行わせる	・ジョブデータ伝送時に接続認証が行われていない脆弱性
		・MFP がジョブデータを受け入れる接続を確立するときに、他システムとの間で交わされる認証手順の通信内容が保護されていないため、攻撃者に ID とパスワードが漏洩し、なりすましをされる	・ジョブデータ伝送時の接続認証の手順が保護されていない脆弱性
		・ジョブデータに利用者を識別する情報が含まれている場合、ジョブデータ内の利用者識別情報を改ざんして別の利用者が出力したかのように見せかける	・他の MFP や他システムから送られてきたジョブデータ内の利用者名を、MFP 本体内で検証できない脆弱性
		・攻撃者は MFP に送信するジョブデータに任意のジョブ制御命令を入力しておくことで、特定の MFP に対して任意のメールアドレスに電子メールを配信させ、攻撃者が特定 MFP を迷惑メール送信サーバとして悪用する	・MFP が受信したジョブデータ内のそれぞれのジョブ制御命令について実行許可が検査されていない脆弱性(対向の MFP やホスト、システムごとなど)
5. 責任追跡性	・ジョブデータを伝送または転送、廃棄した処理の過程で、それぞれの処理がどのモジュールや他システム、どの利用者の指示によって発生したものか確認できず、特定処理の発生原因を確認できない	・メール転送型のファクス伝送処理で、伝送途中にある任意の SMTP サーバで、攻撃者がジョブデータの転送をすりかえて別のファクスイメージを注入しても、どのサーバで書き換えられたのかわからない	・ジョブデータ伝送の経路上で、異なる運用方針を持つ他組織が運用するサーバが介入している脆弱性
		・複数の配信先を指定したジョブデータを MFP に投入したところ、一部の処理が中断して失敗していたが、どの処理が失敗、廃棄されているのかわからない	・ジョブデータに対する複数の処理の処理結果か、失敗や廃棄などの例外的な処理結果が記録されていない脆弱性 ・例外的処理結果の記録がされていても、時刻、利用者、処理内容など十分な内容が記録されていない脆弱性
6. 否	・ジョブデータの処理過程での特定処理がどのモジュールや他システム、どの利用者によって行わ	・LPR では誰でもジョブデータを投入できるので、攻撃者がジョブデータ内に任意の利用者の識別情報を書き込んだ大	・他の利用者の名前、ID・パスワード、セッション情報を再利用して、なりすましができる脆弱性(検証できない脆弱性)

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
認防止	れたか記録があっても立証できない	量のジョブデータを特定の MFP に投入して MFP のサービスを停止させても、ジョブデータ内に書かれた利用者が行ったとはいえず、攻撃者も特定できない	・履歴、監査情報の記録を行うとき、任意の時刻や、任意の利用者名を記録できてしまう脆弱性
7. 信頼性	・ジョブデータが、別のジョブと混同され、イメージデータと宛先が入れ替わってしまう ・イメージデータが破壊され、適当なイメージデータが出力されない ・ジョブの転送処理が悪用され、他システムへの攻撃に利用される	・MFP 内部へのジョブデータの受信、または MFP 外部へのジョブデータの転送中または前後で、攻撃者が並行して特定アドレスへのジョブを MFP に送信し続けると、別のジョブデータの宛先が入れ替り、攻撃者にジョブデータのコピーが送られ、機密の文書が漏洩する	・ジョブデータの受付または配信処理中の競合状態またはリソースが充分に管理されていない脆弱性
		・ある利用者ジョブデータの受付処理を行っている MFP に対して、攻撃者または他システムが受付処理の途中でジョブ制御の範囲外データや、TCP RESET、HTTP の転送データ長を無視したデータなど、例外的なジョブデータや制御を行って、誤ったジョブデータを保存させる、または任意のコードを実行させる	・受け付けたジョブデータの内容の検査が不十分な脆弱性
		・MFP が他システムへの問い合わせを行いながら進められる処理で、大量の不正なジョブデータを与えて、特定の MFP から他システムへ大量の負荷を与えたり、特定の MFP から他システムに不正な問い合わせを行わせて他システムを停止させたり、誤動作させたりする	・受け付けたジョブデータを処理する際に、他システムへの負荷を考慮していない脆弱性

7.6.1 想定される被害の例

1) 継続的に、保護されていない機密の文書が漏洩するか、改ざんされる
2) 継続的に、保護されていないアドレスの一部が漏洩する
3) MFP 使用中か廃棄後に一部の ID、パスワードが漏洩する
4) MFP をほぼ全面的に利用できなくなる(一般利用者)
5) MFP が別の攻撃を実行するホストとして悪用される(任意のコードが実行させられる)

7.6.2 およそのCVSS 2.0 基本評価基準(一部)の影響度

1) AV:攻撃元区分　　ローカル～ネットワーク
2) AC:攻撃条件の複雑さ　高～中
3) Au:攻撃前の認証要否　複数～不要

7.7 管理構成情報

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
1. 機密性	・MFP 本体の構成情報、他システムと通信するための構成情報が漏洩し、資産情報が集中するホストなどの重要な攻撃対象が特定される	・間違えて管理者権限を与えられた保守者が、権限を悪用して MFP 内部の管理構成情報をコピーして持ち出す	・管理者の権限を間違えて保守者に与えることができる脆弱性
		・管理者が構成情報を SD メモリにコピーしたが、紛失し、第三者に管理構成情報が漏洩する	・MFP の構成情報が保護されないまま MFP の外部に保存される脆弱性
		・管理者が MFP に管理者モードで認証後、ログアウトされずそのままになっている MFP コンソールまたは管理者の端末を悪用し、攻撃者が管理者になりすまして管理構成情報を取り出し、漏洩する	・MFP コンソールまたは MFP 上の管理用 Web ページは、管理者の操作が数分以上なくても自動終了しない脆弱性
		・コンソールキーボードと実行基盤の間の USB ケーブルに攻撃者がキーロガーをしかけ、管理構成情報を盗聴する	・MFP 内部のユニット間インタフェース上で通信するデータが保護されていないか、保護が不完全である脆弱性
		・攻撃者が MFP 上で稼動する FTP サーバの脆弱性を攻撃し、MFP 内部で任意のコードを実行し、MFP 内部の特権的操作を実行して管理構成情報をコピーし、管理構成情報が漏洩する	・外部インタフェースから MFP 内部に侵入され特権的操作が実行される脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
2. 完全性	・管理構成情報のうち、セキュリティ機能の使用を無効にさせられ、所定のセキュリティポリシを実現するための構成にできない ・表示される項目が多く、間違いやすい。個々の管理構成情報の項目の間で、設定値の矛盾があっても判定されないため、目標とするサービス条件を達成できない	・管理者が MFP に管理者モードで認証後、ログアウトされずそのままになっている MFP コンソールまたは管理者の端末を悪用し、攻撃者が管理者になりすまして構成情報を変更する	・MFP コンソールまたは MFP 上の管理用 Web ページは、管理者の操作が数分以上なくても自動終了しない脆弱性
		・攻撃者は、管理者がログインしたままのコンソールを悪用して、MFP が他システムと通信するためのプロキシサーバに攻撃者のホストを指定し、機密の文書や他システムと交換される業務情報を継続的に攻撃者に転送させ、機密の文書が漏洩する	
		・攻撃者によってコンソールキーボードが改造または交換され、管理者がコンソールで管理者モード認証をすると、攻撃者が設置したキーボードが任意のキー入力を行い、設定情報を書き換えて登録する	・コンソールキーボードが改造または交換され、コンソールから入力した構成情報を MFP に正しく登録できない
		・管理者が所定のセキュリティポリシを実現する設定を MFP に投入したが、数百項目のうち数項目が間違っていたため通信時データが保護されていなかった。警告メッセージはなかったため継続使用した。攻撃者は MFP の遠隔管理の通信経路のどこかで TCP パケットを盗聴して管理者のパスワードを入手し、継続的な文書の盗聴を行う	・MFP の構成が所定のセキュリティポリシに適合しているか、違反しているかどうか判断しにくい脆弱性 ・違反の検出が行われておらず、違反があっても警告がない脆弱性
		・管理者は取扱説明書のとおりに MFP の不要サービスを停止させ、利用するサービスだけを動作させた。しかし、攻撃者は MFP のサービスポートを調査して取扱説明書に記載がないサービスポートを発見し、そのサービスポートに対して脆弱性調査を行って攻撃し、MFP 内に侵入する	・外部インタフェースから MFP 内部に侵入され特権的操作が実行される脆弱性 ・MFP 内部で動作させていないはずのサービス、または待ち受けていないはずのポートが開いている脆弱性(製品の取扱説明書に記述がなく動作していた場合、利用者による設定が間違っている場合、攻撃者が設定を改ざんした場合)
3. 可用性	・MFP 本体の構成情報、他システムと通信するための構成情報が破壊または削除され、事前に登録しておいた設定構成情報が利用できなくなる ・構成情報を投入できない、更新できなくなる	・MFP の管理コンソールに対して、攻撃者が管理者になりすましてログインし、構成情報を削除する	・外部インタフェースから MFP 内部に侵入され特権的操作が実行される脆弱性
		・攻撃者からの大量リクエストによる過負荷で、管理コンソールを開けなくなり、数十台ある MFP が連続印刷しているのに、すべて遠隔から制御できなくなってしまった	・大量のリクエストを受信すると、コンソールまたは管理モード、保守モードのコンソールが開けなくなる脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
4. 真正性	・MFP 本体の構成情報、他システムと通信するための構成情報が正しい値であるかどうかが確認できない	・ほかの MFP と同じ設定だから設定しておいて、と渡された MFP の設定が、会社のセキュリティポリシに反していた(例: HDD 暗号化機能が on になっていなかった、S/MIME 利用がオフだった)	・MFPの管理構成情報の単体の情報は、その根拠となる情報システムの目標や設計、セキュリティポリシの方針についての情報を持っていない脆弱性
		・MFP に設定して接続させていた他システムのアドレスかポート番号が間違っており、サービスが提供されていなかったか、間違った情報が配布される	・MFP が通信する他システムについて、MFP 内に設定されているアドレスやポート番号などの構成情報が正しいかどうか検証する方法がない脆弱性
5. 責任追跡性	・MFP 本体の構成情報、他システムと通信するための構成情報がどの利用者によって変更・削除されたか、履歴を確認することができない	・運用後数ヶ月で、数十台ある MFP のそれぞれが、少しずつ違う設定になっていたが、複数存在する管理者のうち誰がいつ設定したのかわからず、構成管理の安全対策がとれない	・管理構成情報の書き換え結果が、どの管理者がいつ行ったものか、特定して記録できない脆弱性
6. 否認防止	・MFP 本体の構成情報、他システムと通信するための構成情報を変更・削除した利用者が記録されているが、明確な根拠とともに立証できない	・攻撃者が管理者になりしまして管理構成情報を変更するとき、操作記録に自分以外の利用者名が残るよう、別の管理者の名前を追加して、記録内容をかく乱する	・管理構成情報の操作の記録に利用者名が記録されていたが、その利用者名は利用者から任意の文字列を投入できる脆弱性 [ログが任意の利用者名を受け付ける脆弱性]
		・攻撃者がある管理者になりすましたが、別の管理者も同じ ID とパスワード文字列でログインできるため、どの管理者が実行したかわからない	・管理構成情報の操作の記録に利用者名が記録されていたが、その記録は第三者が改ざん可能な脆弱性 [ログが改ざんされることがある脆弱性]
7. 信頼性	・管理構成情報として入力した情報が適切に表示、保存されない ・入力した管理構成情報のうち一部が保存されなかったり、表示されなかったりする	・管理者パスワードが空欄のまま設定されたが、何も警告表示がなかったためそのままにされ、複数の権限がない利用者が管理者になりすまして MFP の構成情報を勝手に変更し、機密の文書が漏洩する	・受け付けた管理構成情報に、矛盾した設定や範囲外などの間違いがないことを確認する方法がないか、確認していない脆弱性
		・MFP の複数の処理が集中していたときに構成情報を変更しようとしたら、MFP が停止した。起動しなくなるか、起動後も一部機能の動作がおかしい	・ソフトウェアの更新を含む管理構成情報の更新処理を受け付けたときに、処理用のリソースが不足していても処理を実行し、処理の中断または処理後の MFP 内構成情報が予期せぬデータで置き換えられてしまう脆弱性
		・MFPの複数の処理が集中していたときにMFP内のソフトウェアの追加または更新をしようとしたら、MFP が再起動しようとしたあと、まったく起動しなくなる	・受け付けた管理構成情報を処理する際に、MFP 内部または他システムとの間で実行されている処理への負荷を考慮せず、実行中の処理を中断または異常な状態に遷移させる脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
		・管理者が MFP の Web サーバ上にある管理ページを利用して設定変更しようとしたが、利用した Web ブラウザで一部の設定項目の値が一部隠れていたため、セキュリティ機能の一部を有効にできず、攻撃者に機密の文書を盗聴された	・Web ブラウザの違いやバージョンの違いによって、MFP の管理ページの設定項目や説明表示、メニューや入力値のうち一部が表示されないか、間違って表示されるか、わかりにくい脆弱性

7.7.1 想定される被害の例

1) 継続的に、保護されているはずの機密の文書が漏洩するか、改ざんされる
2) 継続的に、保護されているはずのアドレス帳が漏洩する
3) MFP 使用中か廃棄後に証明書、ID、パスワードが漏洩する
4) MFP をほぼ全面的に利用できなくなる(一般利用者、管理者、保守者)
5) MFP が別の攻撃を実行するホストとして悪用される(任意のコードが実行させられる)

7.7.2 およそのCVSS 2.0 基本評価基準(一部)の影響度

1) AV:攻撃元区分　　ローカル～ネットワーク
2) AC:攻撃条件の複雑さ　高～中
3) Au:攻撃前の認証要否　複数～不要

7.8 電子証明書、ID、パスワード、セッション情報(本体内、他システム内)

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
1. 機密性	・MFP 本体の電子証明書用の秘密鍵や、利用者または他システムの ID とパスワードが漏洩し、文書やサーバのなりすましに悪用される	・管理者の ID、パスワードが以下の経路のいずれかで盗聴されて漏洩する: ユニット間のバス上、ネットワーク/遠隔通信、USB・SD メモリ・Bluetooth など機体入出力	・MFP 本体のユニット間インタフェース上の通信データが保護されていない脆弱性
		・攻撃者が管理者になりすまして MFP の管理者モードを利用し、MFP 内の共有文書が攻撃者に漏洩する	・デフォルトの管理者パスワードを誰でも利用できる脆弱性 ・管理者パスワードがつけられていない脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
		・攻撃者が MFP 内に管理者になりすましてログインし、文書の配信経路に攻撃者の宛先を加えられ、継続的に機密の文書が攻撃者に漏洩する	・ID、パスワード、セッション情報を容易に予測できる脆弱性(辞書にある文字列、同じ文字の羅列、IP アドレス、時刻などを使うか、生成された乱数値に偏りがあるなど)
		・攻撃者は MFP と業務システムの間で保護されていない通信を盗聴し、攻撃者は盗聴して得た ID またはパスワード、セッション情報を悪用して、MFP が接続する業務システムに対して、攻撃者が MFP になりすまして接続し、業務システムで扱う情報が攻撃者によって取り出されるか、書き換えられる	・ID、パスワード、セッション情報と、パスワードを含む構成情報が保護されないまま MFP の外部に転送、保存できる脆弱性(他システムとの通信路での漏洩、パスか URL の履歴が渡される、パスワードを保護する認証手順がないか選択されない)
		・MFP 廃棄後に、MFP 内部に残っていた電子証明書、ID、パスワードが第三者に漏洩する	・ID、パスワード、セッション情報と、パスワードを含む構成情報が保護されないままMFPの内部に保存される脆弱性(ストレージからの漏洩、不揮発メモリからの漏洩、履歴・記録からの漏洩) ・電子証明書、ID、パスワードを MFP 内部から完全に消去できない脆弱性
		・MFP の管理者端末が、攻撃者が注入したマルウェアに乗っ取られ、MFP 内部の証明書、ID、パスワード、セッション情報すべてが攻撃者に漏洩する	・管理者のIDとパスワードがあれば、MFP内部のすべての電子証明書、ID とパスワードを取り出すことができ、権限が集中している脆弱性
		・MFP 内部から MFP の電子証明書の秘密鍵を取り出し、その MFP になりすまして他社にファクスを送信し、あたかもその組織が発注したかのような発注書を送付する	・電子証明書の秘密鍵を MFP 内部から取り出せる、または MFP 外部から注入できる脆弱性 (MFP 内部から要求するもの) ・電子証明書の秘密鍵をセキュア IC/TPM に保存していない脆弱性
2. 完全性	・利用者の ID・パスワードが改ざんされ、MFP が提供するサービスを利用者が利用できなくなる ・MFP 本体の電子証明書用の秘密鍵が入替え、改ざんされ、電子証明書を利用するセキュリティ機能が停止または無効にさせられる ・自社または他社の電子証明書が改ざんされ、成りすまされた発信者による文書を信用してしまう	[電子証明書] ・攻撃者が管理者になりすましてログインし、MFP 本体の電子証明書用の秘密鍵を、攻撃者が作った秘密鍵に入れ替え、MFP 上のサーバの SSL/TLS 通信を継続的に盗聴する	・電子証明書の秘密鍵をセキュア IC/TPM に保存していない脆弱性
		・攻撃者は SQL インジェクションを悪用して MFP 内部の管理構成情報を改ざんし、他社宛のメールファクスが、先方で解読できなくなるか、他社から届いたメールファクスの内容を検証できなくなる。場合によって攻撃者からのメールファクスを、特定他社からの文書であると誤認識してしまう	・管理構成情報へのアクセス時の認証がバイパスされる脆弱性 ・特定のクライアント証明書と、宛先を対応付けて管理していない脆弱性(信用しているルート CA から発行されたクライアント証明書をすべて信用してしまう脆弱性)

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
		[ID、パスワード] ・攻撃者は、よくある管理者の ID とパスワードを使って管理者になりすまして MFP にログインし、利用者の ID、パスワードを変更または削除して MFP を利用できなくする	・ID、パスワード、セッション情報を容易に予測できる脆弱性(辞書にある文字列、同じ文字の羅列、IP アドレス、時刻などを使うか、生成された乱数値に偏りがあるなど)
		・攻撃者は MFP と管理者端末の間の保護されていない通信を盗聴して管理者の ID とパスワードを取り出し、管理者になりすまして別の管理者 ID を作成し、以後も継続的に MFP で交換される文書とアドレスが攻撃者に収集される	・ID、パスワード、セッション情報と、パスワードを含む構成情報が保護されないまま MFP の外部に転送、保存できる脆弱性(他システムとの通信路での改ざん、パスワードを保護する認証手順がないか選択されない) ・管理者の ID とパスワードがあれば、MFP 内部のすべての電子証明書、ID とパスワードを追加、変更でき、権限が集中している脆弱性
		・攻撃者は MFP 内部から HDD を取り出して、HDD のコピーを作成し、管理者の ID とパスワードを抽出して取り出す	・ID、パスワード、セッション情報と、パスワードを含む構成情報が保護されないまま MFP の内部に保存される脆弱性(ストレージ上での改ざん、不揮発メモリ上での改ざん)
		[セッション情報] ・MFP で”POP before SMTP 認証”が設定されていると、POP3 または IMAP4 で認証後数分以内の MFP の IP アドレスを発アドレスになりすませば認証なしで SMTP メール送信サービスを利用できてしまうため、攻撃者が MFP になりすましてメールファクスや迷惑メールを送信する	・IP アドレスをセッション情報に利用しているため、容易になりすましされる脆弱性
		・攻撃者が、他の利用者端末が利用中の親展ボックスへのリクエストになりすまして、セッション情報なしか任意のセッション情報を指定するだけで親展ボックスの内容を取り出す	・あるリクエストに対して、その時点で有効な認証、認可済みのセッション情報が照合されていないか照合が不完全である脆弱性
		・攻撃者が、ログアウトした利用者のセッション情報を使って MFP のスキャナボックスへのリクエストを行って、スキャナボックス内の機密の文書が漏洩する	・利用者がログアウトしたあとでもセッション情報が削除されずに利用できる脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
3. 可用性	・MFP 内で生成、登録した電子証明書または秘密鍵が削除され、電子署名やファイル暗号化、サーバ証明書の検証が利用できなくなる ・CA 証明書が削除または改ざんされ、サーバ証明書、文書への署名、コード署名を階層的に検証できなくなる ・対応する CA 証明書が MFP 内にないため、利用者が取得した電子証明書を、MFP が検証できない ・利用者、他システムのための ID・パスワードが削除または改ざんされて MFP を利用できなくなる、または MFP から他システムを利用できなくなる	[電子証明書] ・管理者になりすました攻撃者が MFP の時刻設定を 1 年先に変更し、MFP に格納されている MFP 本体と、宛先メールアドレス、他システム用の電子証明書が無効になり使えなくなる。そのまま MFP は通信路とコンテンツを保護しないまま稼動しつづけ、攻撃者はネットワーク上で容易に盗聴し、文書が漏洩する	・電子証明書には1年程度の有効期限がある脆弱性 ・MFP 内部の電子証明書の有効期限切れがわかりにくい脆弱性
		・MFP 本体のホスト名を変更したが、MFP 内部の証明書を入れ替えなかったため MFP 内部のサーバ証明書が機能停止していた	・利用者用の電子証明書は、証明対象の名称(サーバ証明書ならホスト名かホスト名がないときは直の IP アドレス、クライアント証明書はメールアドレス)が変わったときに無効になる脆弱性 ・MFP 内部の証明書の有効/無効状態がわかりにくい脆弱性 ・MFP がサイトのセキュリティポリシに従って動作しているかわかりにくい脆弱性
		・攻撃者が EMC 攻撃などにより MFP 内部のセキュア IC/TPM 部品か、この部品内のデータだけを破壊し、その MFP のサーバ証明書とクライアント証明書を利用したセキュリティ機能を停止させる	・セキュア IC/TPM を喪失すると、MFP 本体の電子証明書を利用できなくなる脆弱性
		・ある MFP 内部の MFP 本体用の電子証明書が、操作間違いか通信・ネットワークモジュールの脆弱性で侵入され、MFP 本体の電子証明書が作り直されるか改ざんされたため、その MFP 本体の SSL/TLS サーバ機能と S/MIME の保護機能を利用者が利用できなくなる	・MFP 本体の電子証明書が改ざんされると、MFP のセキュリティサービスが利用できなくなる脆弱性
		[ID、パスワード] ・数回以上連続して認証に失敗すると、その ID かパスワードが数分から数時間以上、使えなくなるため、攻撃者が被害者の ID で継続的に認証失敗を繰り返し、被害者の ID を使えなくさせる	・攻撃者が認証を何度でも試行できるネットワーク構成またはアクセス許可の脆弱性
		・攻撃者が MFP の時刻を 1 年早め、MFP 内部の有効期限つきパスワードを無効化させ、自動的にパスワードを更新する機能がない他システムとの通信を停止させる	・パスワードの有効期限切れによりサービスが利用できなくなる脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
		[セッション情報] ・攻撃者が、他の認証済みの利用者のログアウトのリクエストを MFP に送り、その利用者の同意なしでログアウトさせる。再度認証手順を行わせ、ID とパスワードを盗聴または介入する攻撃に利用する	・認証済みのセッション情報が、任意の第三者によって消去できる脆弱性
		・攻撃者が、他の認証済みの利用者のセッションに対して、直前の操作で MFP から提示された秘密の値を指定せず、利用者のなりすましを行うと、その利用者のセッションが無効化される	
4. 真正性	・特定の利用者または他システム用の ID・パスワードについて、権限のある管理者から提供されたものかどうか確認できない ・特定の電子証明書が特定の信頼できる証明書発行局から発行された証明書であるか、確認できない	・管理者の間違いで、一部の MFP 数台にだけ、利用者名と ID の対応が異なっていたため、ある利用者のプリントが別のユーザのスプールボックスに投入されて、権限のないものに機密の文書が漏洩した	・複数の MFP に ID、パスワード文字列を設定するとき、間違って異なる利用者に割り当てられる可能性がある人為的脆弱性
		・ある MFP は外部の認証サーバを利用して、MFP 利用者から ID、パスワード文字列を受け付けて、認証サーバに問い合わせるようになっていた。攻撃者はこれを悪用して、その MFP に特定の ID についてのパスワードを総当りで問い合わせ、MFP に認証サーバに問い合わせて確認させることで、MFP をパスワード解析に悪用した	・MFP が認証応答をする必要がない利用者端末に応答してしまう脆弱性(MFP への接続許可範囲の設定不良、不要なサービスポートの開放) ・MFP 自体または認証サーバが、特定 ID の認証失敗が連続しても、連続して認証要求に応答してしまう脆弱性
		・攻撃者は A 社の名前をかたる偽の証明書を B 社に渡し、B 社は A 社宛のファクスを攻撃者に送ってしまう	・MFP 内で作られた自己署名サーバ証明書は MFP 利用者または他システムに対して信頼できるサイトとして認証されない脆弱性
			・MFP 内部で電子証明書が正しく運用されていない脆弱性(証明書発行手順の間違い、有効期限切れ、所有者識別子[DN]文字列の相違、不適切な CA、秘密鍵の保護が不十分、名前[CN]の存在確認がない、脆弱な暗号方式または暗号鍵の使用)
			・MFP 内部の証明書発行局(CA)証明書(ルート CA 証明書と中間 CA 証明書)に不適切な CA 証明書が混在する脆弱性(Microsoft の場合ルート CA 証明書=320 種類以上、中間 CA 証明書=25 種類以上)
5. 責	・MFP 内電子証明書の生成・登録手順において誰が行ったものか特定できない	・攻撃者は管理者になりすまして MFP にログインし、すでに作成されている MFP 内部の電子証明書を上書きして別の証明書を登録し、MFP 内部で証明書を利用するセキュリテ	・MFP 内部で生成した電子証明書要求書が、どの管理者によって作成されたものか記録がない脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
任追跡性	・利用者または他システムの ID・パスワードについて、新規で MFP に設定したか、変更した操作の履歴を確認できない	ィ機能を停止させるが、記録がないためいつ誰が行ったかわからない	
		・攻撃者は管理者になりすまして MFP にログインし、攻撃者が利用するための ID を追加したが記録がないためいつ誰が行ったかわからない	・MFP 内部で削除、追加、または変更された ID、パスワードについて操作の履歴が記録されていない脆弱性
6. 否認防止	・MFP 内の電子証明書を登録したと記録された、特定の管理者名について、確かにその管理者が実行したものであるということが立証できない ・利用者または他システムの ID・パスワードについて、新規登録・変更・削除を行った利用者を特定する記録があっても、根拠がなく立証できない	・攻撃者が管理者になりすまして MFP の電子証明書を一時的に削除したが、作業記録に偽の情報を追加して別の管理者が操作したように見せかけた、または、操作記録を消去した上で別の管理者が操作したように見せかけた	・操作の記録に利用者名が記録されていたが、その利用者名は利用者から任意の文字列を投入できる脆弱性
			・操作の記録に利用者名が記録されていたが、その記録は第三者が改ざん可能な脆弱性
7. 信頼性	・利用者または他システムの ID・パスワードについて、長さや文字種が適切に入力・表示・保存されない。短くされるか、表示されていない文字列が挿入・追加されている ・ある電子証明書と対応する秘密鍵が正しく対応づけられていないため、電子証明書の検証ができない	・MFP 利用者または他システムから MFP に送られてきた ID、パスワードが予想外の値であったため、MFP 内部で任意のコードが実行されたり、MFP 内部の別のモジュールに命令が注入されたり、MFP 内部の情報を一覧する操作が行われた	・受け付けた電子証明書、ID、パスワード、セッション情報に、矛盾した設定や範囲外などの間違いがないことを確認する方法がないか、確認していない脆弱性 ・MFP が受信または送信する電子証明書、ID、パスワード、セッション情報のデータが予想外の形式で、電子証明書、ID、パスワード、セッション情報を受け入れる MFP 内部のソフトウェアが誤動作、侵入を起こす脆弱性
		・特定の処理中か、大量の負荷があるときに、受信したサーバ証明書または S/MIME メールに添付されている公開鍵証明書の検証が中断しバイパスされる	・電子証明書、ID、パスワード、セッション情報の更新処理を受け付けたときに、処理用のリソースが不足していても処理を実行し、処理の中断または処理後の MFP 内構成情報が予期せぬデータで置き換えられてしまう脆弱性
		・ある特定の処理または大量の処理があると、正しく SSL/TLS 通信ができない、メールファクスで正しい S/MIME 処理ができない	・電子証明書、ID、パスワード、セッション情報を処理する際に、MFP 内部または他システムとの間で実行されている処理への負荷を考慮せず、実行中の処理を中断または異常な状態に遷移させる脆弱性
		・偽の CA 証明書(ルート、中間)か、検証局(OCSP など)が登録され、他システムの偽のサーバのサーバ証明書が有効だとして、誤って検証され、偽のサーバで攻撃者に情報資産を漏洩してしまう	・第三者が発行したルート・中間 CA 証明書のうち一部は信頼できない可能性がある人為的脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
		・以前、別の利用者が使っていた電子証明書か、漏洩があり無効にしなければならないパスワードを更新する機能がないため、古い証明書または ID、パスワードを利用していた以前の利用者またはその情報を入手した攻撃者から、MFP に侵入される	・電子証明書、ID、パスワードを更新する機能がない脆弱性 ・パスワードを定期的に更新していない脆弱性
		・攻撃者は毎日 1-2 回ずつ、特定のユーザのパスワードを予測して、合致するかどうかを MFP に対して試していたところ、数百回の試行でパスワードが合致し、その ID の利用者は攻撃者になりすまされる	・異なる認証手順で利用される異なる利用者名と ID が、サービスの利用者識別や権限認可の際に間違って対応づけられる脆弱性
		・MFP のコンソールから、外部のファイル共有サーバ上の特権ユーザ”Administrator”と同じ利用者名を空のパスワードで登録すると、MFP のコンソールで空のパスワードでログインするだけで外部のファイル共有サーバに、事前に設定された特権ユーザのパスワードを使わないでアクセスできてしまうため、権限のないユーザに機密の文書が漏洩する	

7.8.1 想定される被害の例

1) 継続的に、保護されているはずの機密の文書が漏洩するか、改ざんされる
2) 継続的に、保護されているはずのアドレス帳が漏洩する
3) MFP 使用中か廃棄後に証明書、ID、パスワードが漏洩する
4) MFP をほぼ全面的に利用できなくなる(一般利用者、管理者、保守者)
5) MFP が別の攻撃を実行するホストとして悪用される(任意のコードが実行させられる)

7.8.2 およそのCVSS 2.0 基本評価基準(一部)の影響度

1) AV:攻撃元区分　　ローカル～ネットワーク
2) AC:攻撃条件の複雑さ　高～中
3) Au:攻撃前の認証要否　複数～不要

7.9 正しい時刻

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
1. 機密性	(世界標準時は世界同一なため機密性はない) (MFP 本体内の時刻が世界標準時に比べて何秒ずれているかを示すオフセット値は漏洩しても直接的な脅威はなく危険度は低い: タイムゾーン、サマータイム)	・攻撃者は、MFP の内蔵 Web サーバに問い合わせると、認証なしで MFP 内部の時刻がわかる。MFP 内部の時刻が大幅に狂っていることがわかったときは、時刻に依存したセキュリティ機能が停止してしまっている通信路を特定して盗聴する	・一般に Web サーバは認証なしでサーバ上の時刻を応答する脆弱性
		(現時点で特定の MFP が保持しているタイムゾーン、サマータイムについて特段の機密性への攻撃は見当たらない。これら情報はメールのヘッダ情報などに含まれている)	(現時点でタイムゾーン、サマータイムへの機密性に関する脆弱性は見当たらない)
2. 完全性	・履歴データの時刻が大幅にずれてしまい監査・監視がしにくくなる ・時刻を大幅にずらされて、正しい時刻を使えない	・電子証明書を利用中に、攻撃者が管理者になりすましてMFP の時刻設定を 1 ヶ月先に変更し、SSL/TLS を利用する通信路保護機能と S/MIME でのメール転送文書のコンテンツ保護機能が停止させられ、通信路上で攻撃者に文書を盗聴、改ざんされる	・管理者になりすまされる脆弱性(コンソール、遠隔管理) ・電子証明書には有効期限がある脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
	・MFP 内部の時刻を大幅にずらされ、MFP 内部の電子証明書のほとんどが利用できず、署名の検証、復号、署名による否認防止ができない	・有効期間が定められたライセンス情報を利用中に、攻撃者が NTP 通信に介入して改ざんしたメッセージを MFP に応答し、MFP 内部の時計を同期させないようにした。この結果、MFP のセキュリティ機能を含む、ライセンスが必要な一部または全部の機能が停止させられた	・NTP の通信先を特定していない脆弱性(マルチキャストなど)
		・攻撃者により ARP 偽装された MFP は、偽の NTP サーバと時刻同期を行い、大幅に遅れた時刻に同期させられた	・NTP の通信先との相互認証を行っていない脆弱性
		・攻撃者は犯行時に、MFP の時刻を大幅に狂わせておいたため、該当時刻の攻撃が記録として残らないようにした。記録されたが、保存期間範囲外として翌日の定期処理で削除され、記録が残らなかった	・NTP の時刻同期が成功しているかどうか確認していないか、時刻同期失敗の警告表示がわかりにくい脆弱性
3. 可用性	・正しい時刻を取り出せなくなるか、表示できなくなる	・メールファクスで、不正なタイムゾーン値を受け取ると MFP 内部の時刻応答機能が停止し、セキュリティ機能や操作履歴の記録や監査ログの記録機能が停止させられる。またはライセンス期間を検査されたソフトウェアモジュールの機能が停止させられる	・不正なタイムゾーン値を受け取ると、MFP 内部の時刻応答機能が応答しなくなる脆弱性
		・MFP 内部の時刻が正しい時刻ではないため、セッション情報が常に無効と判定され、Cookie を利用する MFP 上の Web ページが動作しなくなっていた	・リアルタイムクロック用ハードウェアの故障または停止を検出できない脆弱性 ・リアルタイムクロック用の電池を喪失すると、MFP の再起動後から時刻再投入までの間、正しい時刻を得られなくなる脆弱性
		・MFP 内部の時刻が正しくないため、Kerberos の認証が常に失敗しており、集中化した認証サーバによるシングルサインオン機能が利用されておらず、保護されていない通信路上でパスワード入力による認証が実行されていたため、攻撃者にパスワードが漏洩した	
		・MFP 内部のリアルタイムクロック用の電池が切れた状態で MFP を起動後、MFP 内部の時刻が 1970 年のままだったためセキュリティ機能が動作しないまま利用しており、通信路で文書とパスワードが盗聴されていた	
4. 真正性	・MFP 内部の時刻が、どこの時刻ソースに同期しているか確認できない ・NTP の時刻ソースは確かに所定のソースかどうか識別できず、偽ソースを参照してしまう	・管理者は MFP に正しい NTP サーバのホスト名を指定したが、攻撃者が MFP に対して DNS 偽装データを応答し、偽の NTP に接続させた。しかし、MFP は接続した NTP サーバホスト名は表示するが、接続中の NTP サーバの IP アドレスがわからないため、設定したとおりに動作しているのかどうかわ	・NTP の時刻同期ソースを管理していないか表示できない脆弱性 ・NTP サーバとの間の時刻同期のための通信内容を保護していないか、保護が不完全である脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
		からず、MFP の時刻は攻撃者によって狂わされたままとなる	
5. 責任追跡性	・MFP 内部の時刻を同期したときの記録に記載されている時刻ソースのホスト名や時刻機器の名前が確認できない	・特定の MFP から利用中の NTP サーバのうち一部が故障し、異常な時刻と同期するようになったが、履歴がないためどの NTP サーバとの同期を停止すればよいかわからず、対策がとれない	・NTPの時刻同期処理の履歴が記録されていないか、履歴があってもどの同期ソースと同期したか記録されていないなど履歴の内容が不十分な脆弱性
6. 否認防止	・MFP 内部の時刻を同期させた他システムが間違った時刻を提供したことが立証できない	・攻撃者が、ある MFP が利用している NTP サーバのうちのひとつになりすまして、時刻同期応答を返すと、MFP が間違った時刻に同期する。この記録が MFP 内に残されたが、このMFPはNTP通信を保護していなかったため、確かにその NTP サーバが間違った応答をした、ということを立証できない	・NTP サーバとの間の時刻同期のための通信内容を保護していないか、保護が不完全である脆弱性
		・時刻同期の履歴が記録されていたが、その記録は改ざんされる可能性があるため立証に使えない	・時刻同期の記録にホスト名が記録されていたが、そのホスト名は MFP 外部から任意の文字列を投入できる脆弱性［ログが任意のホスト名を受け付ける脆弱性］ ・時刻同期の記録にホスト名が記録されていたが、その記録は第三者が改ざん可能な脆弱性［ログが改ざんされることがある脆弱性］
7. 信頼性	・起動時の時刻が大幅にずれている ・標準時刻に同期し、地域の時刻オフセットに合わせた時刻が出力されない ・時間が経過すると、時刻が標準時刻に同期せずに変動してしまう ・出力された文書を時刻順に並べることができない	・ある中古の MFP でクロック用の電池が切れていたために、他システムに送信されるジョブデータやメール、ファイルの日付が大幅にずれた時刻になってしまう。その結果、日付順の新しい順でジョブ実行記録をソートして表示しているため、攻撃者が不正にコピー転送したジョブ記録が、古いほうに分類されて表示されないため、気がつかない	・MFP 内部のリアルタイムクロック用の電池が切れると、MFP 内部の時刻が 1970 年になる脆弱性
		・ある新古品の MFP で、購入時に時刻合わせをしないまま利用していたところ、管理または監査用の操作履歴やエラーの記録内の時刻情報が大幅にずれることから、他システムの動作記録と参照したときに、履歴の記録として利用できなくなる	・時刻合わせが一度も行われないまま MFP を利用開始できる脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
		・ある管理者が MFP のコンソールを操作して MFP 内の時刻を設定したが、年の数字の入力をひとつ間違えたため時刻が 1 年ずれたまま運用し、正しい有効期限を持つ電子証明書が期間外と判定され、MFP 内で利用されていなかった	・管理者向けの時刻設定表示の文字が小さいか、他の項目と同じ大きさで表示されているため時刻設定を忘れがちな脆弱性 ・時刻設定で、年の数値の入力を間違えたまま気がつきにくい脆弱性(表示文字が小さい、桁が連続してわかりにくい、時間をさかのぼった間違え入力をしても警告がない)
		・指定した NTP サーバと時刻の同期ができず、MFP 内の時刻がずれている	・NTP 手順を適切に処理できない脆弱性
		・MFP を常時通電させ一度も電源オフすることなく 1 年ほど経過するとMFP内部の時刻が異常な値になり、MFP内部のライセンス期間との比較で、MFP の利用権が無効と判定され、その MFP の一部または全部の機能が利用できなくなる	・MFP 内部のクロックがいくつかの数値オーバフローを発生させる脆弱性 (16bit signed/unsigned, 32bit signed/unsigned, 秒/ms/us)
		・2010 年の時点で、30 年間有効な電子証明書を作成し、MFP にインストールしたところ、MFP 内部で日時の比較が適切に処理されず、どうしても電子証明書の有効性を検証できない	・MFP 内部の時刻の処理が 2038 年問題を持つ脆弱性(32bit オーバフロー)
		・MFP に、世界標準時から 5 時間 30 分進んだタイムゾーンと、1 時間進んだサマータイムを設定しようとしても、ファクス文書の時刻には 5 時間 0 分のオフセットしか反映されない	・タイムゾーンとサマータイムに分単位で対応していない脆弱性 ・MFP 内部に世界標準時(GMT)を保持していない脆弱性 ・タイムゾーンとサマータイムの処理が不完全な脆弱性

7.9.1 想定される被害の例

1) 継続的に、保護されているはずの機密の文書が漏洩するか、改ざんされる
2) 継続的に、保護されているはずのアドレス帳が漏洩する
3) MFP 使用中に証明書、ID、パスワードが漏洩する
4) MFP を利用できなくなる(一般利用者、管理者、保守者)
5) 電子ファイルとファクスの文書に間違った日付情報が記録され、間違って扱われる
6) 利用履歴の記録、監査の記録が利用できなくなる

7.9.2 およそのCVSS 2.0 基本評価基準(一部)の影響度

1) AV:攻撃元区分　　ローカル～隣接
2) AC:攻撃条件の複雑さ　高～中
3) Au:攻撃前の認証要否　複数～不要

7.10 原稿、印刷物

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
1. 機密性	・機密情報を含む原稿または印刷物が、第三者に漏洩する	・原稿台や排出トレイに放置された原稿や印刷物を、第三者が読むか、コピー/スキャンして複製を持ち去る	・MFP 本体に第三者が容易にアクセスできる人為的脆弱性 ・原稿台、排紙トレイに原稿または印刷物を置き忘れたことに気づきにくい脆弱性 ・利用者は MFP に処理を指示し、処理中の MFP の前からいったん立ち去ることができる脆弱性 ・ファクス受信または遠隔からの印刷で無条件に紙出力してしまう脆弱性 ・原稿、印刷物などの紙メディアには機密性がない脆弱性 ・原稿台、排紙トレイは利用者なら誰でもアクセスしやすく権限に

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
			よる制限がない脆弱性
2. 完全性	・原稿または印刷物が、置き換えられるか、すりかえられてしまう	・原稿台や排出トレイに放置された原稿や印刷物を、第三者が取り替えて、偽の文書を扱わされる	・原稿、印刷物の紙メディアには機密性がない脆弱性 ・遠隔から印刷すると MFP 本体前にいなくても排紙トレイに印刷物が出力され、排出がわかりにくい脆弱性 ・印刷物に、利用者名などの識別情報がない脆弱性
		・大量コピー中の A さんの処理中に割り込みで十枚程度のコピーをさせてもらったが、同時並行で大量の処理をネットワークで受け付けていたため、MFP の処理が誤り、A さんのコピー出力の一部が割り込み処理の印刷物の中に紛れ込んだ	・多段の割り込み処理によるリソース不足、競合により、フィニッシャへの制御が誤って実行される脆弱性
3. 可用性	・原稿を自動読み込みできない ・印刷物が適切なトレイに排出できない	・攻撃者によって ADF に異物が挿入され、原稿を自動読み込みできない	・MFP 本体に第三者が容易にアクセスできる人為的脆弱性 ・自動原稿読み込み機(ADF)は異物を挿入しやすく、異物がつまると停止する脆弱性 ・給紙装置、紙送り装置は用紙にはさまった異物を巻き込みやすく、紙によっては紙がつまりやすい脆弱性
		・攻撃者が MFP の ADF へのケーブル、フィニッシャへのケーブルを撤去して、ADF とフィニッシャを使用不能にする	・MFP 実行基盤から、ADF への制御ケーブルが不良または切断されると制御ができなくなる脆弱性
		・MFP 近くの強い電磁波の発生源により ADF とフィニッシャが適切に動作せず、利用できない	・MFP 実行基盤から ADF への制御通信が保護されていないか、保護が不完全である脆弱性 ・排紙先のフィニッシャへの制御通信が保護されていないか、保護が不完全である脆弱性
		・MFP 内に装填しておいた用紙とトナーカートリッジが盗難にあい、コピー/印刷/ファクス受信ができない	・MFP 本体の用紙トレイ、トナーカートリッジにアクセスする扉を誰でも開くことができる脆弱性
		・MFP に大量のファクス出力が行われ、用紙とトナーがなくなり、コピー/印刷/ファクス受信ができない	・第三者が MFP 本体にアクセスできる脆弱性 ・MFP の利用者を特定していない脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
			・ファクス受信で無条件に紙出力してしまう脆弱性
4. 真正性	・原稿を、許可された利用者が回収しているかどうかわからない ・ある印刷物が、許可された利用者が回収しているかどうかわからない	・ADF が排出した原稿を、第三者が回収し、機密の文書が漏洩する	・原稿を読み取り台に置き忘れやすく、気づきにくい脆弱性 ・利用者は MFP に処理を指示し、処理中の MFP の前からいったん立ち去ることができる脆弱性 ・読み取り台か排出トレイ上にある原稿、印刷物は誰でも回収できる脆弱性 ・MFP を利用する利用者の認証を行っていない脆弱性
		・コピーの排紙トレイに排出された印刷物を、第三者が回収し、機密の文書が漏洩する	
5. 責任追跡性	・あるスキャンデータやあるファクスデータについて、その元原稿を投入した利用者を特定できない ・ある印刷物について、印刷を行った利用者を特定できない	・ある他社に自社名で偽の注文指示がファクスで届いたが、誰が送ったか特定できない	・MFP を利用する利用者の認証を行っていない脆弱性 ・MFP を利用する利用者の認証結果を操作履歴とともに記録していない脆弱性
		・ある MFP から大量の印刷物が出力されたが、誰が出力したか特定できない	・ある印刷物から、その印刷履歴の記録を MFP 内部から特定するのが難しい脆弱性
6. 否認防止	・あるスキャンデータやあるファクスデータについて、その元原稿を投入した利用者名が記録されていたが、立証する根拠がない ・ある印刷物について、出力した利用者の利用者名が記録されていたが立証する根拠がない	・攻撃者が架空の領収書/請求書をスキャンして保存回覧していたが、監査のあと指摘を受けると、それは別人がスキャンしたデータだと主張され、立証できない	・MFP 利用者の操作記録に利用者名が記録されていたが、その利用者名は MFP 外部から任意の文字列を投入できる脆弱性
		・ある大量のカラー印刷物について、出力記録に利用者名がある利用者に確認したが、自分ではないと主張され、立証できない	・MFP 利用者の記録に利用者名が記録されていたが、その記録は第三者が改ざん可能な脆弱性
7. 信頼性	・大量の原稿や印刷物を正しい順序で出力できない ・割り込み処理を多段で行うと間違った出力や保存が行われる ・印刷物を指定どおりのイメージと仕上げにできない: 出力されたイメージや配置が異なる、適切なトレイに排出できない、印刷物が指定どおりの数で	・数千部の印刷を開始したが、攻撃者からの多数のリクエストを受け付けることで、一部の印刷物のイメージ配置、ページ順、綴じが不良になり、廃棄処分となり、納期も遅れて損害が発生した	・MFP が大量の処理を受けつけると、MFP 内部のリソースが不足するか、一部または全部のジョブデータの一部が破壊、混同され指示どおりの処理ができなくなる脆弱性
		・数千部の印刷を開始したが、攻撃者からの電磁波妨害によりすべての印刷物の綴じが不良になり、廃棄処分となった。数十万枚の用紙と大量のトナーが無駄になる	・原稿台、排紙トレイは利用者なら誰でもアクセスしやすく権限による制限がない脆弱性
		・穴あけのゴミの滞留、補充用のホチキスの針の間違いによる大量印刷の失敗	・穴あけのゴミの滞留、補充用のホチキスの針の誤挿入がわかりにくい

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
	出力されない、部単位のソートができない、ホチキス止めができない、穴あけできない、ホチキス/穴あけの場所が違う、折りができないか間違っている	・用紙トレイの中に厚みが異なる用紙が数枚混入したため、大量印刷の途中で用紙が詰まったり、複数枚吸い込まれたりして印刷不良になった	・用紙の厚みは人からはわかりにくい脆弱性

7.10.1 想定される被害の例

1) 断続的に機密の文書が漏洩するか、改ざんされる
2) 断続的にアドレス帳が漏洩する
3) MFP の一部機能を利用できなくなる(一般利用者)
4) トナー、用紙などの消耗品が無駄に消費される

7.10.2 およそのCVSS 2.0 基本評価基準(一部)の影響度

1) AV:攻撃元区分　ローカル
2) AC:攻撃条件の複雑さ　高～低
3) Au:攻撃前の認証要否　複数～不要

7.11 MFP 内共有ファイル

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
1. 機密性	・機密情報を含むファイルが、MFP 本体内の共有フォルダから第三者に漏洩する	・攻撃者がリクエスト引数を変化させ、MFP 内部のパスワードを含む構成管理ファイルのパス名を突き止める	・MFP 内部の共有フォルダへのリクエストの内容の検査が不十分で、非公開のフォルダやファイル名を読み取られる脆弱性、内部命令を注入されて認証と権限の検査をバイパスされる脆弱性
		・攻撃者がリクエスト引数に SQL インジェクションを仕掛けて、どのような制限にも影響なく、機密のファイルを取り出す	
		・機密のファイルが MFP 内部の共有フォルダの公開フォルダにあったため、第三者に機密のファイルが漏洩した	・機密の文書が、間違って公開されたフォルダに配置されてしまう人為的脆弱性
		・機密のファイルが機密のフォルダにあったが、攻撃者がゲストの資格または一般利用者の資格でファイルを入手できる状態だったため機密の情報が不適切な資格者に漏洩した	・適切な利用者を認証し、適切な利用権限が設定されていない脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
			・適切な利用者を認証し、適切な利用権限を割当処理できない脆弱性
		・MFP 内部の共有フォルダを検索する機能を使うと機密の文書名が誰にでも提示され、場合によってはそのままダウンロードができるため機密の文書が第三者に漏洩する	・検索すると非公開のファイル名が漏洩する脆弱性 ・検索経由でファイルを開くとセキュリティがバイパスする脆弱性
		・MFP 内部の共有フォルダ内のファイルをコンソールで表示したり、SD メモリに出力したり、紙に印刷、ファクスに送信、ボックスに配信、PC など他システムのフォルダに配信、メールで配信、他システムの URL へ送信する場合、認証不要になることを利用して、資格がない利用者に機密の情報が漏洩する	・出力先の種類によってセキュリティ機能をバイパスできる脆弱性
		・攻撃者が管理者になりすまして、MFP 内部の共有フォルダを含めてバックアップを作成して入手し、共有フォルダ内の機密の文書が漏洩する	・管理者が MFP の内部共有ファイルを閲覧できる脆弱性 ・MFP 内部共有ファイルが暗号化などで保護されてない脆弱性
		・保守業者が、ストレージ装置を交換するときに不良品の HDD を回収して持ち帰り、機密の文書を含む共有フォルダ内のファイルを取り出す	・ストレージ内のデータが暗号化などで保護されていないか、保護が不完全である脆弱性
2. 完全性	・MFP 本体内の共有フォルダにあるファイルが、置き換えられるか、すりかえられてしまう	・攻撃者から、MFP 内部の DB エンジンに対して SQL インジェクションやコマンドインジェクションを注入され、ファイルが書き換えられてしまう	・MFP 内部共有ファイルへのフォルダ名やパス名、ID 番号、属性などのリクエストの内容の検査が不十分
		・MFP 内部のリソースあふれか競合状態を発生させるようなリクエストを発生させながら、特定文書が投入されたときに一部データのすり替えを行う	・MFP の大量処理中にリソース不足または競合によりデータのすりかえが発生してしまう脆弱性
		・負荷が多いと、検索用のインデックスや文書管理用のデータベースの一部または全部が破壊される	
		・攻撃者は MFP の共有ファイルサーバの認証手順に対し、手順の途中で「認証完了」のメッセージを送信するか、認証の途中でリクエストを送信し、認証手順のバイパスが成功してしまう	・MFP 内部共有ファイルへの認証をバイパスできる脆弱性
		・攻撃者は管理者端末と MFP の共有ファイルサーバの間の保護されていない通信を盗聴して、とりだしたセッション情報を悪用して共有ファイルサーバに対して管理者になりすまし、管理者特権によって MFP 内部の共有ファイルをいくつ	・MFP 内部共有ファイルと他システムの間の通信が保護されていない脆弱性 ・管理者が MFP 内部の共有ファイルを無制限に書き換えまたは

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
		でも別のファイルに入れ替える	追加できる脆弱性
		・攻撃者は管理者になりすまして、バックアップを取り出し、改ざんしてから書き戻し(レストア)して MFP 内共有ファイルを改ざんする	・MFP 内部共有ファイルが暗号化などで保護されてないか、保護が不完全である脆弱性
		・攻撃者はストレージ部品を抜き取り、ストレージ部品内部のセクタを書き換えて、ストレージ部品を MFP 内部に戻し、MFP 内部の共有ファイルを改ざんする	・ストレージ内のデータが暗号化などで保護されていないか、保護が不完全である脆弱性
3. 可用性	・MFP 本体内の共有フォルダのサービスが利用できなくなるか、非常に長い応答時間がかかるようになる(ファイル取り出し、書き込み、更新、一覧)	・攻撃者が MFP 内部の DB エンジンに対して SQL インジェクションを投入して、MFP 内部のファイルか、DB 内の文書情報を削除される	・MFP 内部の共有ファイルへのリクエストの内容の検査が不十分でリソース不足または処理が停止、遅延する脆弱性
		・攻撃者が、MFP に対して認証が失敗するリクエストを大量に送信し、MFP がほとんどの利用者の認証をしばらくの間ロックアウトしてしまう	・攻撃者からの要求で認証失敗が連続すると正規利用者がロックアウトされる脆弱性
		・MFP 内部の共有ファイルの処理内で処理の無限ループが発生するようなリクエストを注入され、MFP の反応が遅くなるか、停止する	・大量のリクエストや処理の滞留により共有フォルダ上のサービスが利用できなくなる脆弱性(処理メモリ、CPU 処理量、バス帯域の圧迫、一時ファイル、文書ファイル、ログファイルによるディスクの圧迫)
		・MFP が大量のリクエストを受けて、MFP 内の共有ファイルサービスが停止する	
		・MFP 内部のストレージ装置が抜き取られるか故障し、MFP 内部の共有ファイルがすべて利用できなくなる	・ストレージ装置のいずれかまたは全部を喪失すると MFP 内部の共有フォルダが利用できなくなる脆弱性
4. 真正性	・MFP 本体内の共有フォルダにあるファイルの一部または全部が、どの利用者が作成したものかわからない	・MFP 内部の共有ファイルにファイルを作成しても利用者属性が記録されず、攻撃者はいつでも利用者不明のファイルを作成できる	・MFP 内部の共有フォルダへの作成者による電子署名が行われていない脆弱性 ・MFP 内部の共有ファイルの利用者属性が、文書内容の作成者を示していない脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
		・攻撃者は異常に長いユーザ名を指定したジョブファイルを MFP に送り、MFP 内部の共有ファイル管理ソフトがユーザ属性情報を記録せずにファイルを保存してしまう	・MFP 内部の共有ファイル作成時に利用者識別機能や識別情報の記録処理がバイパスされる脆弱性 ・MFP 内部の共有ファイルサーバが入力値を充分に検査していない脆弱性 ・MFP 内部の共有ファイルサーバの利用者識別機能の動作状態に関する脆弱性(動作させたはずが動作していないか、動作できない。動作しているかどうかわかりにくい)
5. 責任追跡性	・MFP 本体内の共有フォルダにある特定のファイルが、誰が作成し、誰が閲覧したか、履歴をたどれない	・攻撃者はディレクトリトラバーサル攻撃を実行して、MFP 共有ファイルをすべて閲覧し、重要な文書を作成している人物の部署と名前を特定し、さらに次に攻撃を行う。しかし、MFP の運用者による監視と監査ではこの攻撃者の行動を検出することができず、攻撃を防止できない	・MFP 内部の共有ファイルの操作履歴が記録されていない脆弱性
6. 否認防止	・MFP 本体内の共有フォルダにある特定のファイルを、作成、更新、閲覧した記録に利用者名が残っていたが、否認されても立証できない	・運用者は、ある利用者が大量のファイルを閲覧している記録を確認したが、その利用者の閲覧記録は、簡単に注入または改ざんできる記録で、本人のものではなかった	・操作の記録に利用者名が記録されていたが、その利用者名は利用者から任意の文字列を投入できる脆弱性 ・操作の記録に利用者名が記録されていたが、その記録は第三者が改ざん可能な脆弱性
7. 信頼性	・投入したはずの文書ファイルか、取り出した文書ファイルの内容の一部が別のファイルかジョブの内容と置き換わっている ・投入したはずの文書ファイルが、取り出そうとしてもなくなっている ・任意のコードが実行させられる	・攻撃者が MFP 内部のリソースあふれか競合状態を発生させるようなリクエストを発生させながら、特定文書が投入されたときに一部データのすり替えを行う	・大量処理によるリソース不足、競合で誤って処理される脆弱性
		・攻撃者が MFP 内部のリソースあふれか競合状態を発生させるようなリクエストを発生させると、一部文書の保存処理が不完全になる。そのため一般利用者からは保存できたように見えるが、保存できていないため取り出せない	・多段の割り込み処理によるリソース不足か競合により、誤って処理される脆弱性
		・攻撃者が不正なファイル属性値を指定する命令を注入し、MFP 内部の共有ファイルサーバにスタックオーバフローを起こさせ、任意の命令を実行させる	・MFP 内部共有ファイルサーバの入力値の検査不足により、任意のコードが実行させられる脆弱性(パス名、ID、属性値、ファイルデータ)

7.11.1 想定される被害の例

1) 継続的に、保護されているはずの機密の文書が漏洩するか、改ざんされる
2) 継続的に、保護されているはずの一部のアドレスが漏洩する
3) MFP 使用中に証明書、ID、パスワードが漏洩する
4) MFP の共有ファイル機能を利用できなくなる(一般利用者、管理者、保守者)
5) MFP が別の攻撃を実行するホストとして悪用される(任意のコードが実行させられる)

7.11.2 およそのCVSS 2.0 基本評価基準(一部)の影響度

1) AV:攻撃元区分　　ローカル～ネットワーク
2) AC:攻撃条件の複雑さ　高～中
3) Au:攻撃前の認証要否　複数～不要

7.12 利用履歴、監査記録

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
1. 機密性	・利用履歴または監査記録に含まれる、宛先、発番号、サーバアドレスなどのアドレスが 1 件以上漏洩する	・攻撃者がリクエスト引数に SQL インジェクションを仕掛けて、どのような制限にも影響なく、利用履歴を取り出した	・MFP へのリクエストの内容の検査が不十分で、非公開のフォルダやファイル名を読み取られる脆弱性、内部命令を注入されて認証と権限の検査をバイパスされる脆弱性(コマンドインジェクション)
		・利用履歴が機密のフォルダにあったが、攻撃者がゲストの資格または一般利用者の資格でファイルを入手できる状態だったため利用履歴が不適切な資格者に漏洩した	・利用履歴、監査記録に関する利用者の認証と権限が適切に設定されていないか、適切に割当処理ができない脆弱性
		・利用履歴が MFP 内部の公開フォルダにあったため、第三者に利用履歴が漏洩した	・機密の情報を、公開されたフォルダに配置してしまう人為的脆弱性
		・検索する機能を経由して利用履歴にアクセスすると、権限なしでダウンロードができるため利用履歴が第三者に漏洩する	・検索経由でファイルを開くとセキュリティがバイパスする脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
		・利用履歴をコンソールで表示するか、SD メモリに出力するか、紙に印刷、ファクスに送信、ボックスに配信、PC など他システムのフォルダに配信、メールで配信、他システムの URL へ送信する場合、認証不要になることを利用して、資格がない利用者に利用履歴が漏洩する	・出力先の種類によってセキュリティ機能をバイパスできる脆弱性
		・攻撃者が管理者になりすまして、利用履歴を含めてバックアップを作成して入手し、利用履歴が漏洩する	・管理者に利用履歴と監査記録のすべてを取り出せる権限が集中している脆弱性
		・保守業者が、ストレージ装置を交換するときに不良品の HDD を回収して持ち帰り、利用履歴が取り出されて漏洩する	・ストレージ内のデータが暗号化などで保護されていないか、保護が不完全である脆弱性
2. 完全性	・利用履歴または監査記録が記録されていても内容の一部が改ざんされている	・攻撃者は SQL インジェクションやコマンドインジェクションにより、利用履歴と監査履歴の特定レコードの時刻か利用者名、処理内容の記録を改ざんする	・不十分な入力の検査、数値データによる脆弱性
		・攻撃者は利用履歴をかく乱するため、他の利用者が攻撃者と同じ操作をしたかのような記録を、MFP 内部の利用履歴記録モジュールに注入した	・利用履歴、監査記録の追加または削除操作に関する利用者の認証と権限が適切に設定されていないか、適切に割当処理ができない脆弱性
		・攻撃者は認証なしで利用履歴を更新した	
		・攻撃者は一般利用者の一人として認証を受け、利用履歴を更新した	
		・攻撃者は書き込み可能なフォルダに配置されていた利用履歴を改ざんした	・利用履歴が、利用権限不要なフォルダに公開されている脆弱性
		・攻撃者は MFP に不正な形式の利用履歴リクエストか、認証が完了する前に認証を完了させるかリクエストを送り、MFP は認証なしで利用履歴を更新した	・MFP へのリクエストの内容の検査が不十分で、権限なしで内部データを削除または追加、更新できてしまう脆弱性 ・リクエストの受付インタフェースでセキュリティ機能がバイパスされる脆弱性
		・攻撃者は管理者になりすまして MFP 内部の利用履歴を更新した	・管理者が利用履歴を改ざんできる脆弱性
		・攻撃者がストレージのバックアップを取り出し、利用履歴を改ざんしてから書き戻した	・ストレージ内のデータが暗号化などで保護されていないか、保護が不完全である脆弱性
		・攻撃者はストレージを抜き出して利用履歴を改ざんしてストレージを元に戻した	

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
3. 可用性	・利用履歴または監査記録の表示または確認、検査ができなくなる	・攻撃者は SQL インジェクションにより利用履歴と監査履歴をすべて削除する	・不十分な入力の検査、数値データによる脆弱性
		・攻撃者はコマンドインジェクションにより、MFP 内部にある履歴の記録用プロセスを強制終了させる	
		・攻撃者は MFP に大量のリクエストを送り、その MFP 内部で利用履歴が記録されないようにした上で、攻撃を行う	・大量のリクエストや処理の滞留により利用履歴が記録されなくなる脆弱性(処理メモリ、CPU 処理量、バス帯域の圧迫、一時ファイル、文書ファイル、ログファイルによるディスクの圧迫)
		・攻撃者は管理者になりすまして利用履歴の記録を停止させる、または MFP の入力脆弱性を利用して利用履歴の動作を停止させるか、記録処理をしないまま正常終了するよう、実行コードを書き換える	・利用履歴を記録するソフトウェア機能が停止またはバイパスされる脆弱性
		・攻撃者は認証なしで利用履歴を削除した	・利用履歴の削除について適切に認証されていない脆弱性
		・攻撃者は一般利用者の一人として認証を受け、利用履歴を削除した	・充分な権限がなくても利用履歴を削除できる脆弱性
		・攻撃者は書き込み可能なフォルダに配置されていた利用履歴を削除した	・削除または書き換え可能な場所に利用履歴を記録する脆弱性
		・攻撃者はストレージを抜き出して別のコンピュータからストレージにアクセスし、利用履歴を削除してストレージを元に戻した	・ストレージ上の利用履歴データが保護されていない脆弱性
4. 真正性	・利用履歴または監査記録の削除について、誰が行ったものか、正しい時刻かどうかわからない	・MFP 内部の利用履歴を削除しても利用者属性が記録されないため、特定の管理者は攻撃を行ったあとでいつも利用履歴を削除する	・利用履歴の操作時に利用者を識別していない脆弱性
		・MFP 内部の利用履歴を操作した記録については、攻撃者が任意の利用者名を指定して追記させ、どの管理者が利用履歴を削除したかわからないようにする	・利用履歴の操作時に追加記録される利用者名が、任意の値にできる脆弱性
5. 責任追跡性	・利用履歴または監査記録の削除について、誰が行った処理の記録か、特定できない	・昨日まではあった利用履歴が削除されていても、どの管理者が行ったのかわからない	・利用履歴の削除操作自体は記録していない脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
6. 否認防止	・利用履歴または監査記録の削除について、特定の利用者が実行したものと記録があっても、記録の根拠がなく立証できない	・利用履歴の削除を行った利用者として、ある管理者の利用者名が記録されていたが、攻撃者が任意の文字列を投入すると追記できるようになっていたため、どの管理者が行ったのかわからなかった	・利用履歴の操作の記録に利用者名が記録されていたが、その利用者名は利用者から任意の文字列を投入できる脆弱性
		・利用履歴の削除を行ったと記録がある、ある管理者の名前は、利用履歴の改ざんによる別名の利用者名だったため、どの管理者が削除を行ったか特定できない	・利用履歴の操作の記録に利用者名が記録されていたが、その記録は第三者が改ざん可能な脆弱性
7. 信頼性	・利用履歴または監査記録が正しい時刻と真正な利用者名、正しい処理名とともに記録されていない ・実際に行った利用の履歴の一部または全部が記録されていない	・ある MFP は再起動すると管理者が手動で時刻合わせをするまで MFP 内部の時刻が 1970 年になるため、攻撃者は攻撃の前に MFP に不正なパケットを送って再起動させ、それから MFP に攻撃を行うことで、攻撃中の記録を古い記録として残させる。管理者が時刻を合わせると、古い時刻の攻撃の記録は自動的に削除され、管理者は攻撃の確認ができなくなる	・MFP が正しい時刻を保持していない脆弱性
		・攻撃者は、ある MFP が利用履歴と監査情報をあとから修正できる機能があるため、これを悪用して MFP に攻撃を加えたあと、すぐに記録を消去した	・MFP の既存の利用履歴記録を変更か修正できる脆弱性
		・ある MFP は監査記録の利用者名が常に同じになるため、攻撃者が MFP を攻撃して機密の文書を取り出した記録を特定できない	・MFP が利用履歴の記録時に、識別済みか認証済みの利用者情報を記録していない脆弱性
		・MFP の一部の利用履歴だけは、数値データの範囲やメッセージ長の長さの異常により、間違った処理名や、メッセージの一部しか記録されないため、攻撃者の攻撃手法を分析できない	・MFP の一部の利用履歴は、間違った処理名や値が記録されている脆弱性
		・攻撃者はサーバに異常に長いユーザ名を MFP に送り、MFP 内部の履歴記録機能がユーザ属性情報を記録しないようにする	・利用履歴または監査記録に記録される利用者名は利用者認証の結果を反映していない脆弱性(常に固定か、不定の値)

7.12.1 想定される被害の例

1) 継続的に、利用履歴が漏洩する。または本体か部品の廃棄後に利用履歴が漏洩する
2) 継続的に、一部のアドレスが漏洩する
3) MFP 使用中か廃棄後に ID、パスワードの一部が漏洩する
4) 利用履歴が改ざんされる
5) 利用履歴を参照できなくなる

7.12.2 およそのCVSS 2.0 基本評価基準(一部)の影響度

1) AV:攻撃元区分　　ローカル～ネットワーク
2) AC:攻撃条件の複雑さ　高～中
3) Au:攻撃前の認証要否　複数～不要

7.13 MFP 利用課金情報

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
1. 機密性	・課金情報、利用量情報が、権限のない者に漏洩する	・攻撃者がリクエスト引数に SQL インジェクションを仕掛けて、適切な権限なしで、課金情報を取り出す	・不十分な入力の検査、数値データによる脆弱性
		・課金情報が公開フォルダにあったため、第三者に課金情報が漏洩する	・機密の文書を、公開されたフォルダに配置してしまう人為的脆弱性
		・課金情報が、攻撃者がゲストの資格または一般利用者の資格でファイルを入手できる状態だったため課金情報が不適切な資格者に漏洩する	・適切な利用者を認証し、適切な利用権限を割当処理できない脆弱性
		・課金情報に関する検索を行うと課金情報の文書名が誰にでも提示され、場合によってはそのままダウンロードができるため課金情報が第三者に漏洩する	・MFP へのリクエストの内容の検査が不十分で、非公開のフォルダやファイル名を読み取られる脆弱性、内部命令を注入されて認証と権限の検査をバイパスされる脆弱性
		・検索する機能を経由して課金情報にアクセスすると、権限なしでダウンロードができるため第三者に漏洩する	・検索経由でファイルを開くとセキュリティがバイパスする脆弱性
		・課金情報をコンソールで表示したり、SD メモリに出力したり、紙に印刷、ファクスに送信、ボックスに配信、PC など他システムのフォルダに配信、メールで配信、他システムの URL	・出力先の種類によってセキュリティ機能をバイパスできる脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
		へ送信する場合、認証不要になることを利用して、資格がない利用者に課金情報が漏洩する	
		・攻撃者は、管理者がログインしたままになっている管理者端末を悪用して、課金情報を含めて MFP 内部データのバックアップを作成して入手し、スプールされていたジョブデータの機密の文書と、ID、パスワード、セッション情報が漏洩する	・管理者か保守者になりすまされる脆弱性 ・ストレージ内のデータが暗号化などで保護されていないか、保護が不完全である脆弱性
2. 完全性	・MFP 利用課金情報の一部または全部が改ざんされ、利用者の適切な課金情報を収集できないか、利用者に適切な請求が行われない	・攻撃者は SQL インジェクションを悪用して、MFP の利用課金情報を 30%少ない値に書き換え、保守業者に支払う毎月の課金を 30%減少させた	・不十分な入力の検査、数値データによる脆弱性 ・MFP 利用課金情報をコマンドインジェクションによって書き換えできる脆弱性
		・攻撃者は管理者になりすまして、MFP の利用課金情報をゼロに書き換えていた	・MFP 利用課金情報が管理者によって書き換えできる脆弱性
		・攻撃者は保守者になりすまして、MFP の利用課金情報を 2 倍に書き換えていた	・MFP 利用課金情報が保守者によって書き換えできる脆弱性
		・攻撃者は MFP の遠隔保守用の課金集計 API を特定し、利用課金情報をゼロに書き換えていた	・利用者に公開されていないインタフェース（遠隔保守インタフェース)の脆弱性 ・認証が行われていない外部インタフェースの脆弱性
		・攻撃者は MFP の遠隔保守用の http proxy 上に追加の処理を挿入し、課金報告メッセージ内の課金数値をゼロに書き換えるようにして、保守業者への従量課金を継続的に毎月ゼロにした	・遠隔保守インタフェースの通信データが保護されていないか、保護が不完全である脆弱性
		・攻撃者は、MFP 内部にある EEPROM を部品交換して、利用済みの利用課金情報を書き込み、過大な料金が請求されるようにした	・MFP 内部のハードウェアを容易に交換できる脆弱性
		・攻撃者は、MFP 内部にある、利用課金情報を書き込むストレージ部品を撤去または破壊し、課金情報が記録されないまま利用を継続した	・利用課金情報を格納するストレージがなくても動作してしまう脆弱性
3. 可	・MFP の利用があったのに利用課金情報が加算されなくなる	・攻撃者は、MFP 内部にコードを注入し、MFP をよく利用する時間帯だけ、利用課金を加算する処理をバイパスさせ、保守者に支払う課金を 6 割減少させた	・利用課金を加算する処理が停止またはバイパスされる脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
用性	・保守機能または遠隔保守機能の機能が無効またはアクセス不能にさせられ、課金情報をとりだせなくなる	・攻撃者は間違った保守者認証を連続的に実行し、保守業者がログインできないようにした	・保守者認証で間違ったパスワードが数回連続すると保守者モードが一定時間ロックされる脆弱性(コンソール認証、遠隔認証ともに)
		・攻撃者は管理者になりすまして課金情報を消去した	・管理者が課金情報を消去できる脆弱性
4. 真正性	・MFP 利用課金情報が正しい値かどうかわからないため、MFP 利用課金情報が改ざんされていてもわからない	・攻撃者は MFP の課金集計 API を特定し、マイナスの数値を注入して、利用課金情報を減らし、課金を減額した	・利用者に公開されていないインタフェースが動作してしまう脆弱性 ・利用課金情報を交換する外部インタフェースで認証が行われていない脆弱性
		・攻撃者はMFPの課金集計APIを悪用し、過大な利用実績値数値を注入して、利用者課金情報を実際よりも 60%増大させ、課金を増額させた	・利用課金情報を加算するソース情報を識別、特定していない脆弱性
5. 責任追跡性	・MFP 利用課金情報が初期化されるか、予想外の数値に改ざんされていたとしても、その原因を確認できない	・その MFP 内部のソフトウェアには利用課金情報の操作履歴を記録する機能がオプションで、搭載されていなかった	・利用課金情報の操作履歴が記録されていない脆弱性
		・そのMFP内部の利用課金情報の操作履歴の記録を行うソフトウェアには利用者名を記録する機能がなかった	・利用課金情報の操作履歴の記録に、時刻、利用者名、操作種別のいずれかが記録されていない脆弱性
6. 否認防止	・MFP 利用課金情報の一部または全部が消去・改ざんされたのに、特定の保守者が行った、ということを立証できない	・攻撃者は利用課金情報を削除したあと、遠隔保守業者が削除したかのような操作履歴を API 経由で注入し、原因利用者を特定しにくくした	・操作の記録に利用者名が記録されていたが、その利用者名は利用者から任意の文字列を投入できる脆弱性［ログが任意の利用者名を受け付ける脆弱性］
		・攻撃者は利用課金情報を削除したあと、管理者になりすまして MFP のバックアップ機能とレストア機能を利用して、遠隔保守業者が削除したかのような操作履歴に書き換え、原因利用者を特定しにくくした	・操作の記録に利用者名が記録されていたが、その記録は第三者が改ざん可能な脆弱性［ログが改ざんされることがある脆弱性］
7. 信頼性	・長大で多数のジョブデータが集中するなど、特定の条件下で MFP の利用課金情報が適切な値でなくなり、正しい課金ができなくなる	・攻撃者は MFP 内部に特定の競合状態が発生するように、長時間かかるジョブを投入し続け、利用課金情報が加算されないように、別の大量のジョブを実行させた	・競合状態、リソース管理に関する脆弱性
		・攻撃者は犯行時に、MFP の時刻を大幅に狂わせておいたため、該当時刻の攻撃が記録として残らないようにした1記録されたが、保存期間範囲外として翌日の定期処理で削除され、記録が残らなかった。(「正しい時刻」にも同じ記載	・MFP が正しい時刻を保持していない(「正しい時刻」と同じ記載)

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
		・1,000 部の印刷を 4 台の MFP に分散して処理したところ、4,000 部の課金が加算され、過大な利用課金請求があった	・他の MFP に分割したジョブデータの印刷を二重に課金する脆弱性(不具合) – 課金の条件が明示されていない脆弱性
		・利用課金情報をもとにした課金は何円かわからず、印刷するたびに調べているため時間がかかる	・利用課金の単価と、ジョブデータ単位の課金量が表示されない脆弱性

7.13.1 想定される被害の例

1) 継続的に課金情報が漏洩する
2) 継続的に課金情報が改ざんされる
3) 継続的に課金情報が参照できなくなる(保守者)

7.13.2 およそのCVSS 2.0 基本評価基準(一部)の影響度

1) AV:攻撃元区分　　ローカル～ネットワーク
2) AC:攻撃条件の複雑さ　高～中
3) Au:攻撃前の認証要否　複数～不要

7.14 通信システム(スイッチ、DHCP, DNS, NTP を含む)

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
1. 機密性	・MFP が通信するための配線またはコネクタが露出しており、容易に別の装置を挿入して盗聴される 通信用の無線電波が容易に盗聴される ・スイッチングハブまたは VLAN に、物理的制限も認証もなしで容易に接続でき、盗聴、第三者中継を行われる	・攻撃者が、装置を通信システムのケーブルの間に挿入し、以下の保護されていない通信を盗聴してメールサーバ用の ID とパスワードを収集、記録する 保護されていない通信: IPv4, IPv6, DHCP, ARP, ICMP, ICMPv6, LLMNR, Rendezvous, TCP, UDP, UPnP, DNS, TELNET, SNMP, SMTP, POP3, IMAP4, SIP, FTP, HTTP, SMB, LPR, RAW9100, IPP など	・MFP と他システムとの間の通信内容が保護されていないか、保護が不完全

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
	(通信機器には DNS、DHCP,NTP を含む)	・MFP の USB プリンタポート、USB メモリポート、USB 認証ユニットポートが、TCP/IP で伝送され、遠隔地に延長されていたが、通信内容が保護されていなかったため、機密の文書、認証用のカード番号などが盗聴され、攻撃者に漏洩する	・USB/SCSI など非 IP インタフェースの伝送データを IP 化して伝送するときの脆弱性
		・攻撃者が路上から、MFP が利用する無線 LAN の WEP 鍵を解読し、MFP が通信する外部の共有ファイルサーバとの ID とパスワードを FTP プロトコルから取り出す。攻撃者は MFP になりすまして共有ファイルサーバ内の文書を取り出す	・無線 LAN の WEP 暗号化が必要な暗号強度に満たない脆弱性
		・攻撃者は遠隔のスイッチングハブ上で、VLAN 配布プロトコルを使って MFP 専用の VLAN に所属する Ethernet ポートを作成し、MFP と同一の VLAN に接続する。その後攻撃者は MFP のデフォルトゲートウェイになりすまし、第三者中継攻撃を実行する	・制限されていないタグ VLAN の脆弱性
		・MFP を間違った VLAN に接続したか、IPsec の構成が間違っていたため、ネットワーク上で MFP が隔離されておらず、一般利用者と同じネットワークに接続し、保護されていない通信が盗聴されていた	・通信システムの複数または多段の通信経路のどこかで構成か設定が間違っている脆弱性(Ethernet, VLAN, IPsec, VPN)
2. 完全性	・MFP の保護されていない通信が改ざんされる ・USB/SCSI などの汎用インタフェースで第三者中継され、印刷・スキャン・ファクスのイメージデータやアドレスが改ざんされる (通信機器には DNS、DHCP,NTP を含む)	・DNS サーバからのホスト名解決応答が保護されていなかったため攻撃者によって改ざんされ、以後の MFP からのリクエストが、攻撃者が用意したホストへと誘導される	・MFP と他システムとの間の通信内容が保護されていないか、保護が不完全
		・攻撃者が、装置を通信システムのケーブルの間に挿入し、保護されていない通信に介入してメールサーバ用の ID とパスワードを改ざんする その他の保護されていない通信: IPv4/IPv6, DHCP, ARP, ICMP, ICMPv6, LLMNR, Rendezvous, TCP, UDP, UPnP, DNS, TELNET, SNMP, SMTP, POP3, IMAP4, SIP, FTP, HTTP, SMB, LPR, RAW9100, IPP など	

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
		・DHCP/DHCPv6 サーバからの応答メッセージが保護されていなかったため、改ざんされた DHCP 応答メッセージを受信した MFP はそれ以後、攻撃者が用意したデフォルトゲートウェイを常に使うようになった	・MFP と他システムとの間の通信で相互認証が行われていない脆弱性
		・MFP の USB プリンタポート、USB メモリポート、USB 認証ユニットポートが、TCP/IP で伝送され、遠隔地に延長されていたが、通信内容が保護されていなかったため、攻撃者が介入し、ジョブデータが改ざんされて、印刷部数が常に一部多く改ざんされていて、機密の文書が漏洩した	・USB/SCSI など非 IP インタフェースの伝送データを IP 化して伝送するときの脆弱性
		・攻撃者が路上から、MFP が利用する無線 LAN の WEP 鍵を解読し、MFP が通信する、保護されていない外部の共有アドレスサーバとの通信に介入し、グループアドレスに攻撃者を追加する改ざんを行い、攻撃者は MFP が特定のグループに送信するファイルのコピーをメールで得ることになり、機密の文書が漏洩する	・無線 LAN と WEP 暗号化保護方式の脆弱性
		・MFP を間違った VLAN に接続したか、IPsec の構成が間違っていたため、ネットワーク上で MFP が隔離されておらず、一般利用者と同じネットワークに接続し、保護されていない通信が改ざんされていた	・通信システムの複数または多段の通信経路のどこかで構成か設定が間違っている脆弱性(Ethernet, VLAN, IPsec, VPN)
3. 可用性	・通信機器の盗難または配線の切断や盗難、端子の抜けにより、MFP を利用できなくなる ・通信機器の動作停止により MFP を利用できなくなる ・通信システムの構成間違いにより、MFP 自体に通信できないか、他システムと MFP が通信できないために MFP を利用できない (通信機器には DNS、DHCP,NTP を含む)	・攻撃者は MFP に接続された Ethernet ケーブルを抜いて、MFP のサービスのほとんどを停止させる	・MFP は通信システムが介在しないと利用できない脆弱性
		・スイッチングハブまたは無線 LAN アクセスポイントの故障により MFP のサービスが停止する	
		・VLAN または IPsec、VPN の構成を間違うか、所定の VLAN ポートか所定の Ethernet ポートに接続しなかったため、MFP がサービス提供できない	・通信システムの複数または多段の通信経路のどこかで構成か設定が間違っている脆弱性(Ethernet, VLAN, IPsec, VPN)
4. 真	・通信相手の機器が所定のセキュリティ要件で特定された機器かどうか、確認できない	・数十台の MFP が利用する NTP サーバとの通信で、認証が行われていなかったため、偽の NTP サーバを利用させられる	・MFP と他システムとの間の通信で相互認証が行われていない脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
正性	(通信機器には DNS、DHCP,NTP を含む)	・DNS サーバからの応答に偽のホスト名情報が紛れ込んでいて、MFP の外部共有フォルダにファイルを書き込むときに偽のホストに誘導される	
		・偽の DHCP から偽の DNS サーバの IP アドレスを注入される	
5. 責任追跡性	・偽のソースアドレスで通信が行われても、どの機器からの通信だったのか特定できない (通信機器には DNS、DHCP,NTP を含む)	・MFP の時刻が大幅に変化する現象があったが、記録がないため、どの NTP サーバの不具合かわからない	・MFP が通信システム上で設定した IP アドレス構成を履歴として記録していない脆弱性
		・MFP が偽の IP アドレスを注入されていたが、どの DHCP サーバから注入されていたか特定できず、対策を立てられない	
		・DNS の応答に脆弱性を攻撃するデータが含まれていたが、記録がないためどのホストが応答または注入したものか特定できない	
6. 否認防止	・通信相手を特定するためのアドレスについて記録があっても、対向システムの管理者が否認すると立証できない (通信機器には DNS、DHCP,NTP を含む)	・通信の記録に利用者名は含まれているが、任意の利用者名を投入できるため証拠にならない	・接続の記録に利用者名が記録されていたが、その利用者名は利用者から任意の文字列を投入できる脆弱性
		・通信の記録はどのホストからでも注入可能なため、攻撃者からの記録が混じり、不具合の原因を特定できない	・操作の記録に利用者名が記録されていたが、その記録は第三者が改ざん可能な脆弱性
		・IPsec で接続していた通信相手との間で、グループ鍵を使っていたため他のホストでもなりすまし可能だったため、接続記録から攻撃があったと見られる利用者端末を特定できなくなる	・通信を許可する認証がなりすまし可能である脆弱性
7. 信頼性	・通信において送信したデータが他のデータと混同されて受信されるか、送信したデータの一部が欠落して受信されることで正しい動作ができない (通信機器には DNS、DHCP,NTP を含む)	・通信システムの負荷が容量を超えると、IP パケットの欠落が発生する。その結果 MFP は、再送処理を行うが、MFP 内部でも処理負荷が高まることから、競合やリソース不足が発生し、処理を中断したり不完全なまま処理が実行されたりする	・競合またはリソース不足による脆弱性
		・攻撃者が DNS、DHCP、NTP サーバに複雑な多種類のリクエストを送り、これらサーバ内の競合により一部のパケットや応答メッセージが欠落したり入れ替わったりし、MFP は適切な応答を受信できない	・他システム上の脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
		・攻撃者が DNS、DHCP、NTP サーバのいずれかに、既知の脆弱性を利用してサーバ内部に侵入し、任意のコードを実行し、MFP は適切な応答を受信できないか、上記サーバが MFP など関連する他システムを攻撃する	

7.14.1 想定される被害の例

1) 継続的に、保護されていない機密の文書が漏洩するか、改ざんされる
2) 継続的に、保護されていないアドレス帳が継続的に漏洩する
3) 継続的に、保護されていない通信路上で MFP を使用中に ID、パスワードが漏洩する
4) 保護されていない通信路上で不正な時刻を受け取り、ひとつ以上のデータ保護機能か通信保護機能が停止させられる
5) MFP をほぼ全面的に利用できなくなる(一般利用者、管理者、保守者)

7.14.2 およそのCVSS 2.0 基本評価基準(一部)の影響度

1) AV:攻撃元区分　　ローカル～隣接
2) AC:攻撃条件の複雑さ　高～中
3) Au:攻撃前の認証要否　複数～不要

7.15 遠隔管理システム

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
1. 機密性	[遠隔管理機能の利用時] ・権限のない遠隔管理機能の利用 ・MFP内部に保存されている、機密を含む共有ファイル、複数のアドレスが、遠隔管理機能を経由して漏洩する [遠隔管理システムそのもの]	・攻撃者は、MFP のアドレス帳を送受信する通信のうち保護されていない通信を盗聴し、攻撃者にアドレス帳の内容が漏洩する: アドレス帳の登録・更新、アドレス帳のバックアップ、単発のファクス配信またはメール配信またはサーバ配信を定義するためのアドレス帳同期、複数配信処理を定義するためのアドレス帳同期、他システムからの制御用アドレス帳参照	・他システムと MFP の通信が保護されていないか、保護が不完全である脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
	・外部管理システムが攻撃され、外部にあったアドレス帳またはバックアップデータが攻撃者に漏洩する	・攻撃者は、構成管理サーバ上の脆弱性を突いて侵入またはリクエスト強要し、他システム上に保存されている、MFP で利用するアドレス帳と同じデータ、または MFP のバックアップデータを入手する	・他システム自体の脆弱性
		・攻撃者が管理サーバ、認証サーバ、監視サーバのいずれかに、既知の脆弱性を利用してサーバ内部に侵入し、任意のコードを実行し、MFP は適切な応答を受信できないか、上記サーバが MFP など関連する他システムを攻撃する	
2. 完全性	[遠隔管理機能の利用時] ・MFP に投入または取り出すアドレス、構成情報が改ざんされる	・攻撃者は通信路上で ARP 偽装を使って遠隔管理端末と MFP の間の通信に介入し、MFP に投入されるアドレスを改ざんし、攻撃者のアドレスを追加し、以後継続的に機密の文書の盗聴を行う	・他システムと MFP の通信が保護されていないか、保護が不完全である脆弱性
	[遠隔管理システムそのもの] ・外部の管理システム上の構成情報が改ざんされ、複数の MFP が予期せぬ動作をする	・MFP の遠隔保守を行うインタフェースのポートはデフォルトで閉じているはずが開いており、このポートに攻撃者が接続して遠隔保守機能を悪用する	・MFP の一部の遠隔サービスインタフェースまたは API に、管理者権限で命令を実行できる API が残って稼動している脆弱性
	・認証サーバの一部が置き換えられるか、認証データの一部が改ざんされてなりすましされるか、サービスが停止させられる	・MFP の遠隔バックアップ機能の CSRF 脆弱性を悪用して、攻撃者が管理者または保守者の Web ブラウザに特定の URL を開かせ、攻撃者が任意の管理機能を実行する	・管理者の端末ブラウザ、保守者の端末ブラウザに対する CSRF リクエスト強要攻撃が成功する脆弱性
3. 可用性	[遠隔管理機能の利用時] ・攻撃者によって MFP に破壊された設定が投入され、MFP を利用できなくなるか、動作不良になる	・攻撃者が、保護されていない構成システムから MFP への構成変更指示のメッセージを改ざんし、破壊された構成データが MFP 内部に登録され、MFP が停止するか、所定の動作をしなくなる	・他システムと MFP の通信が保護されていないか、保護が不完全である脆弱性
	[遠隔管理システムそのもの] ・認証サーバの応答が停止させられ、MFP を利用できなくなる ・監視サーバが停止させられ、稼動情報が得られなくなる	・攻撃者は利用者端末になりすまして、MFP の遠隔管理インタフェースにアクセスし、何度も ID、パスワードによる認証を試す。すると MFP 用の認証サーバは連続したログイン失敗を検出して、しばらく(数分間)、管理者のログインを禁止する。この作業を連続して行うことで、その他 MFP の管理機能を停止させる	・管理者の認証失敗が連続すると、管理者がログインできなくなる脆弱性 ・どの端末からでも管理者の認証要求を実行できる脆弱性
	・構成管理サーバが停止させられ、新しいアドレス	・攻撃者は監視サーバの脆弱性を突いて、監視サーバを停止させることで、MFP の稼動情報が収集されないようにする	・遠隔管理システム自体の脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
	を追加できなくなる。アドレス帳を検索できなくなる	・攻撃者は構成管理サーバの脆弱性を突いて、共有アドレス帳を削除し、MFP に空のアドレス帳を同期させ、MFP でアドレス選択ができなくする	
4. 真正性	[遠隔管理機能の利用時] ・遠隔管理システムからの認証応答、アドレス帳応答、設定構成変更の要求、保守要求が、認められた遠隔管理システムからのものではなかった [遠隔管理システムそのもの] ・特定の MFP に対して、ある管理サーバや認証サーバが正しい応答を行っているか確認できない	・認証サーバが正しい認証サーバであるか、MFP 側から検証を行っていないシステムで、攻撃者は偽の認証サーバを用意して、MFP と通信させ、別の悪意の端末を利用者になりすましさせて MFP を悪用する	・MFP と遠隔管理システムとの間で、相互認証が行われていない脆弱性
		・攻撃者は MFP の監視サーバになりすまし、MFP に対して大量の監視要求メッセージを送信し、MFP を過負荷状態にする	・MFP と遠隔管理システムとの間の通信が保護されていない脆弱性 ・MFP と遠隔管理システムとの間で相互認証が行われていない脆弱性
		・攻撃者は管理者に特定の URL を開かせ、管理者の利用端末に CSRF 攻撃を行い、MFP のバックアップデータを取得させ、攻撃者が用意した詐取可能なフォルダに転送させ、攻撃者が MFP のバックアップデータを入手する	・管理者の端末ブラウザ、保守者の端末ブラウザに対する CSRF リクエスト強要攻撃が成功する脆弱性 (他システムと MFP の間の認証後のステートレスな通信(HTTP など)で、重要な操作や機能に関する要求が、その直前の操作に特有な情報と関連づけがあることを検査していない)
		・攻撃者はアドレス帳サーバから MFP への応答メッセージを通信路上で改ざんし、宛先アドレスを攻撃者のアドレスに変更し、機密の文書を攻撃者が入手する	・MFP と遠隔管理システムと間の通信が保護されていないか、保護が不完全である脆弱性
		・攻撃者が既知の脆弱性を利用して、認証サーバに任意のコードを実行させて制御を乗っ取り、MFP が要求する遠隔管理システムの認証がすべて正しいと応答させられる。そのため、MFP は偽の管理サーバからの接続を受け入れてしまう	・認証サーバそのものの脆弱性
5. 責任	[遠隔管理機能の利用時] ・MFP が遠隔管理システムから要求された処理または遠隔管理システムからの応答について、MFP 内部に記録されているはずなのに記録されていな	・アドレス帳への通信履歴は MFP 内にも、アドレス帳サーバにも記録されていなかったため、攻撃者がアドレス帳データを外部から検索要求して引き出し、外部の業者に販売していたことがわからなかった	・遠隔管理システムとの通信履歴が記録されていない脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
追跡性	い [遠隔管理システムそのもの] ・遠隔管理システムが、どの MFP にどのような要求を行い、応答結果の成否、失敗理由などの履歴が遠隔管理システムの側に記録されていないため、不具合時に原因調査ができない	・監視サーバの記録に一部欠けている部分があったが、遠隔管理システムとの通信履歴に時刻がなかったため、監視記録がなかった期間に MFP がどのような処理を行っていたかどうかが特定できず、対策を立てられない	・遠隔管理システムとの通信履歴の記録に、時刻、利用者名、操作種別のいずれかが記録されていない脆弱性
		・管理権限で構成変更を行う構成サーバから MFP への要求を行ったが、MFP には要求が見当たらない。構成サーバがいつなんという要求を送信したか確認しようとしたが、構成サーバ内での履歴がなく確認できず、対策を立てられない	・MFP 内部に記録する遠隔管理システムとの通信履歴の内容のうち、逆引きされたホスト名は DNS で偽装される脆弱性
6. 否認防止	[遠隔管理機能の利用時] ・遠隔管理システムからの要求を処理したときに、MFP 内に記録される認証サーバ、監視サーバ、管理サーバの名前が、改ざんされたか、なりすましされたものではないことを立証できない [遠隔管理システムそのもの] ・遠隔管理システム上に、どの MFP に要求したか、どの MFP から要求が来たか記録するとき、MFP のホスト名やユーザ名が改ざんされたか、なりすましされたものでないことを立証できない	・ある管理者が MFP 内部のバックアップデータを不正に取り出したという、遠隔管理システムから MFP の管理機能を利用した記録があったが、MFP 内部の操作履歴には任意の値を注入できるか、改ざん可能な脆弱性があったため、その管理者の操作だと特定できない	・操作の記録に遠隔管理システムの IP アドレスが記録されていたが、その利用者名は利用者から任意の文字列を投入できる脆弱性
		・MFP を遠隔から監視するシステムに、特定の MFP が正常稼動していた、という記録があったが、この状態通知は攻撃者による偽の通知だったため、攻撃者から攻撃を受けていたときの異常通知から警報を出せない(SNMP)	・操作の記録に遠隔管理システムの IP アドレスが記録されていたが、その記録は第三者が改ざん可能な脆弱性
7. 信頼性	[遠隔管理機能の利用時] ・MFP が遠隔管理システムとの処理を正しく行えない ・MFP は複数の遠隔管理システムからの要求を、受付順序どおり、または優先順序どおり処理できず、前後の入れ替えがある ・受け付けた処理を全部処理せず、一部だけ欠落した。要求の一部が別の要求に置き換わるか、一部の処理を重複して処理する ・受け付けた一部の要求は繰り返し処理され止まらなくなる	・管理者端末のブラウザ上で、攻撃者が送ったメールの本文内にあった URL を開いたところ、不正な JavaScript コードが実行され、その管理者がログイン済みだった共有アドレス帳サーバのアドレス内容がすべて攻撃者にコピーされる	・管理者の端末ブラウザ、保守者の端末ブラウザに対する CSRF リクエスト強要攻撃が成功する脆弱性
		・ある MFP へのリクエスト数が一定以上になると、認証サーバから MFP への認証応答を元のリクエストに正しく対応させられなくなり、第三者に意図しない権限を与えてしまう。攻撃者はこれを利用して管理者権限を奪取する	・複数の利用者が同時に同じ MFP を設定変更することにより構成情報が破壊される脆弱性
		・あるタイプの保留中ジョブデータが増えると、管理サーバから MFP 内部のアドレス帳への変更操作で、削除と追加の順で処理される指示が、追加と削除の順で処理されるため、追加されずに残ってしまう。残ったアドレスは管理外になるため、攻撃者はこれを利用して別の MFP 利用者への偽メッセージを送る	・競合状態、リソース管理に関する脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
	[遠隔管理システムそのもの] ・遠隔管理システム自体の異常により MFP が正しい処理を行えない ・認証サーバが利用者 ID を取り違えるか、処理中のパスワードの一部が欠落するために MFP を利用できなくなる ・監視サーバが異なる MFP を監視してしまうため結果がおかしい ・アドレス帳共有サーバ内のアドレスデータの対応がずれて欠落しているため適切なアドレスが得られない	・長大なジョブデータの処理中に、MFP 内のリソース不足から、アドレス帳の更新が途中で中断してしまう	
		・複数ある MFP 内部の時刻がばらばらだったため、複数 MFP に分散処理した出力がすべて終わったかどうか監視サーバから確認するのに、さらに数時間かかる	・MFP が正しい時刻を保持していない
		・遠隔管理システム自体の脆弱性を突いて攻撃者が遠隔管理システム上に侵入することにより、遠隔管理システム上で正しい順序で所定の内容の応答をすることができなくなり、MFP が正しく動作しなくなる	・遠隔管理システム上で MFP を操作する管理者にも、MFP 内部のすべての構成管理情報と ID、パスワードなどを変更でき、権限が集中している脆弱性
		・ある一般利用者の ID とパスワードが漏洩したが、この一般利用者は管理者権限を持ち、管理者用にも同じ ID とパスワードを使っていたため、攻撃者が遠隔から管理者として MFP に接続し、すべての構成情報と ID とパスワードをだましとり、別のホストへの攻撃に利用しながら、機密の文書とアドレスを販売した	
		・ある MFP に対して SNMP で監視を行っていたが、ジョブデータのバイトカウンタが 32bit であふれたあと不定値になり監視できない、またはジョブデータのデータ量のカウントのはずがほかのパケットのデータ量も加算されていて比較ができない	・MFP が SNMP で応答する MFP 内部の状態値が間違っている脆弱性(測定方法の間違い、測定対象か応答対象値が入れ替わっている、不適切な型変換や数値変換が行われている)

7.15.1 想定される被害の例

1) 継続的に、保護されているはずの機密の文書が漏洩するか、改ざんされる
2) 継続的に、保護されているはずのアドレス帳が漏洩する
3) MFP 使用中に証明書、ID、パスワードが漏洩する
4) MFP の異常状態を検出できないか、検出が大幅に遅れる
5) MFP の利用履歴が記録されなくなる
6) MFP を利用できなくなる(一般利用者、管理者、保守者)

7.15.2 およそのCVSS 2.0 基本評価基準(一部)の影響度

1) AV:攻撃元区分　　ローカル～ネットワーク
2) AC:攻撃条件の複雑さ　高～中
3) Au:攻撃前の認証要否　複数～不要

7.16 一般利用者端末

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
1. 機密性	・利用者端末内で実行されるドライバソフトウェアで保存される認証用の ID・パスワードが漏洩する ・利用者端末内で保存されるスプールファイルが保護されていないため、スプールファイルに含まれる文書とアドレスが漏洩する ・利用者端末から定期的に行われる MFP への状態確認問合せにより、MFP のアドレスと機種が特定される	・攻撃者から利用者端末へのリクエスト強要攻撃により、利用者が過去に送信した履歴が残っていた文書を任意のアドレスに印刷またはファクス、配信させられ、攻撃者に漏洩する	・他システムと MFP の間の認証後のステートレスな通信(HTTP など)で、重要な操作や機能に関する要求が、その直前の操作に特有な情報と関連づけがあることを検査していない脆弱性(CSRF リクエスト強要など)
		・攻撃者は利用者端末上の MFP 用ドライバ API、または MFP 用 SDK API の脆弱性を突いて、任意のコードを実行させ、任意のアドレスへ機密の文書のコピーを送信させる	・メーカが提供する MFP 用ドライバソフトウェア自体、または MFP 用 SDK ライブラリ自体の脆弱性（数値処理、情報漏えい、入力の確認、セキュリティ機能、競合状態、リソース管理）（プリントドライバ、ファクスドライバ、スキャンドライバ）
		・攻撃者は利用者端末上にすでに動作しているマルウェアを操作し、MFP 用のドライバに設定してあるアドレスとパスワード、または機密の文書を含むスプールファイルを入手する	・利用者端末の MFP ドライバ用に設定された電子証明書、ID、パスワードが保護されずに保存される脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
		・攻撃者は、利用者端末と MFP の間の保護されていない通信を盗聴して、MFP の IP アドレス、型番、利用者の ID、パスワードを収集し、攻撃の準備を行う	・他システム(他の MFP、利用者端末、蓄積・外部処理、遠隔管理システム)と MFP の間の通信が保護されていない脆弱性
		・利用者端末内に、MFP 以外のアプリケーションの脆弱性を突いたマルウェアが動作しており、プリントとスキャンの入出力を含めて、MFP と交換するファイルのコピーが攻撃者に転送されていた	・利用者端末自体の脆弱性（利用者端末の OS かアプリケーションが更新されておらず既知の脆弱性を持つなど）
2. 完全性	・利用者端末で実行されるドライバソフトウェアそのもの、または実行中のソフトウェアの状態が改ざんされ、攻撃者により任意のコードが実行される ・利用者端末内に保存されたドライバソフトウェア用に設定された構成情報、認証情報が改ざんされる ・利用者端末と MFP の間のメッセージが改ざんされる	・攻撃者は利用者端末用の MFP 用ドライバ API または SDK 用 API の脆弱性を突いて、特定の脆弱性を攻撃するコードを利用者に実行させ、利用者端末の制御を奪い、ジョブデータを改ざんする	・メーカが提供する MFP 用ドライバソフトウェア自体、または MFP 用 SDK ライブラリ自体の脆弱性（数値処理、情報漏えい、入力の確認、セキュリティ機能、競合状態、リソース管理）（プリントドライバ、ファクスドライバ、スキャンドライバ）
		・攻撃者は利用者端末にマルウェアを感染させ、利用者端末上の MFP 用のドライバの構成情報と ID・パスワードを書き換え、利用者が MFP に送信する機密の文書を攻撃者にも送信させる	・利用者端末の MFP ドライバ用に設定された電子証明書、ID、パスワードが保護されずに保存される脆弱性
		・攻撃者は MFP と利用者端末の通信路上で ARP 偽装による介入や偽の無線 LAN AP による介入、偽のプロキシサーバによる介入により、MFP と利用者端末の間のジョブデータの改ざんを行い、攻撃者に機密の文書のコピーを送る	・他システムと MFP の通信が保護されていないか、保護が不完全である脆弱性
		・利用者端末内に、MFP 以外のアプリケーションの脆弱性を突いたマルウェアが動作しており、プリント時のスプールファイルが改ざんされて、攻撃者にもプリントイメージのコピーが配信されていた	・利用者端末自体の脆弱性（利用者端末の OS かアプリケーションが更新されておらず既知の脆弱性を持つなど）
3. 可用性	・利用者端末内で実行されるドライバソフトウェアが削除されるか破壊されていて MFP を利用できない ・利用者端末内に保存されている、ドライバソフトウェアの構成情報または認証情報が削除または改ざんされて MFP を利用できない	・利用者端末にインストールした MFP 用ドライバがすでに破壊されており、MFP を利用できない	・利用者端末用の MFP 用ドライバのインストールファイルが壊れているかインストールできない脆弱性
		・攻撃者は利用者端末用の MFP 用ドライバ API または SDK 用 API の脆弱性を突いて、利用者端末の制御を停止または暴走させ、MFP を利用できないようにする	・メーカが提供する MFP 用ドライバソフトウェア自体、または MFP 用 SDK ライブラリ自体の脆弱性（数値処理、情報漏えい、入力の確認、セキュリティ機能、競合状態、リソース管理）（プリントドライバ、ファクスドライバ、スキャンドライバ） ・利用者端末の MFP ドライバ用に設定された電子証明書、ID、パスワードが削除される脆弱性
		・利用者端末が侵入され、MFP 用ドライバが削除されて MFP を利用できない	
		・利用者端末が侵入され、MFP 用ドライバの設定情報が削除または破壊されて MFP を利用できない	

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
		・攻撃者は一般利用者端末と MFP の間の通信中のセッションに対して、セッション終了メッセージ(無線 LAN，TCP，SSL/TLS)を挿入してセッションを強制終了させる	・他システムと MFP の通信が保護されていないか、保護が不完全である脆弱性
		・攻撃者は利用者端末上のサービスポート、または MFP 上のサービスポートに多量のリクエストを送り、サービスを停止させる	・利用者端末用のサービスポート上での競合またはリソース不足の脆弱性
		・利用者端末内に、MFP 以外のアプリケーションの脆弱性を突いたマルウェアが動作しており、特定の MFP 以外へのプリントができないようになっており、特定の MFP にプリントすると、攻撃者にコピーが転送されるようになっていた	・利用者端末自体の脆弱性（利用者端末の OS かアプリケーションが更新されておらず既知の脆弱性を持つなど）
4. 真正性	・利用者端末上にインストールするドライバソフトウェアが、これから利用しようとしている MFP 用の正しいソフトウェアであるかどうかわからない ・特定の MFP 用のドライバをインストールしようとしている利用者端末が、MFP を利用してよい端末かどうかわからない	・ある利用者端末上にインストールされた、ある MFP 用のドライバソフトウェアは、マルウェアが同梱されたものだった。特に警告表示がなかったため、利用者はそのまま利用を継続し、機密の文書が漏洩することにつながった	・利用者端末用の MFP 用ドライバまたは MFP 用ユーティリティのインストールファイルが正しいファイルかどうか判定できない脆弱性
		・ある利用者端末は、既知の脆弱性がある未修正の OS を利用しており、すでにマルウェアに感染していたが、MFP 用のドライバをインストールされ、MFP へのサービス停止攻撃が実行されてしまった	・利用者端末自体の脆弱性（利用者端末の OS かアプリケーションが更新されておらず既知の脆弱性を持つなど）
5. 責任追跡性	・利用者端末の内部のソフトウェアを、正しい利用者が正しい手順で利用したか、さかのぼって確認できない	・ある他社に自社名で偽の注文指示がファクスで届いたが、誰が送ったか特定できない	・MFP を利用する利用者の認証を行っていない脆弱性
		・ある MFP から大量の印刷物が出力されたが、誰が出力したか特定できない	・MFP を利用する利用者の認証結果を操作履歴とともに記録していない脆弱性
6. 否認防止	・ドライバソフトウェアが記録として残した操作記録、処理記録の内容に、改ざんがありえないなどの根拠を示して立証できない	・利用者端末の OS 上で、ドライバソフトウェアが利用されるたびにドライバが行う操作記録の処理において、操作記録には任意の文字列を投入できるなどの改ざんが可能なため、利用履歴にある情報の立証ができない	・操作の記録に利用者端末のホスト名が記録されていたが、その利用者名は利用者から任意の文字列を投入できる脆弱性
		・利用者端末上に記録されている使用履歴は、利用者端末上に感染したマルウェアによって改ざんされており利用できなかった	・操作の記録に利用者端末のホスト名が記録されていたが、その記録は第三者が改ざん可能な脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
7. 信頼性	・利用者端末内のドライバソフトウェアと関連するアプリケーションがデータを取り違えるか、欠落させてしまう ・ドライバソフトウェアの制御が乗っ取られ、異なるデータや異なる利用者からのジョブとしてすりかえられてしまう	・特定のデータが含まれるプリントを実行すると、プリンタドライバの脆弱性により、期待どおりに印刷できないか、別のジョブデータやプリンタ内ファイルの内容が混入した印刷物が出力されて、機密の文書が漏洩する	・メーカが提供するドライバソフトウェア自体の脆弱性（数値処理、情報漏えい、入力の確認、セキュリティ機能、競合状態、リソース管理）（プリントドライバ、ファクスドライバ、スキャンドライバ）
		・攻撃者がプリンタドライバの脆弱性を突いて、プリンタドライバ内の制御を乗っ取り、プリンタドライバの設定を書き換えて、プリントが実行されると必ず攻撃者にもプリントの複製が送られるようにされ、継続的に機密の文書が漏洩する	

7.16.1 想定される被害の例

1) 継続的に、保護されているはずの機密の文書が漏洩するか、改ざんされる
2) 継続的に、保護されているはずのアドレス帳が漏洩する
3) MFP 使用中に ID、パスワードが漏洩する
4) MFP を利用できなくなる(一般利用者)
5) 一般利用者端末用の MFP ドライバソフトウェアが解析され、脆弱性が発見される

7.16.2 およそのCVSS 2.0 基本評価基準(一部)の影響度

1) AV:攻撃元区分　　ローカル
2) AC:攻撃条件の複雑さ　高～中
3) Au:攻撃前の認証要否　複数～不要

7.17 蓄積・外部処理(スプーラ、共有フォルダ、メール、業務システム)

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
1. 機密性	・蓄積・外部処理サーバが行う通信が保護されていないために通信路上で盗聴され文書が漏洩する。 ・ある MFP が特定の処理のために他システムから取り出した機密の文書を、その MFP 上で漏洩させてしまう ・蓄積・外部処理サーバ(文書を蓄積するサーバやプロキシサーバ、コンテンツの変換処理などを行うサーバ)で、文書が漏洩する	・攻撃者は、蓄積・外部処理サーバと MFP の間の保護されていない通信を盗聴し、機密の文書を含むジョブデータを入手する。攻撃者は入手したデータを販売し、機密の情報が漏洩する	・他システムと MFP の間の通信が保護されていないか、保護が不完全である脆弱性
		・多数の拠点に一度に文書の配信を行う際、複数メーカの MFP と複数機種の MFP を使っていたため、一部の MFP に配信するための通信が保護されていなかった。攻撃者は保護されていない通信だけを盗聴して、機密の文書が漏洩する	
		・一部の一般利用者は、MFP 外部の共有フォルダでは権限がないファイルでも、MFP 上に配信を要求すると閲覧できるようになり、部外者に機密の文書が漏洩する	・他システムと MFP の間で、ファイルの所有者や権限などの属性が異なる脆弱性
		・あるサイトでは MFP でスキャンされたイメージデータは常に外部の共有フォルダの特定の公開フォルダに格納されるため、似たような文書名の違う資料と取り違えて機密の文書が権限のない者に漏洩する	・機密の文書を公開フォルダに置いてしまう人為的脆弱性
		・多数の拠点に一度に文書の配信を行う際、複数メーカの MFP を使っていたために用語が異なり、配信、親展、ボックス、送信、プリント、メール、サーバ送信、URL 送信などの機能を誤って使用し、不要な印刷出力を行うか、不適切なサーバへの文書のコピーを行っていたため、機密の文書が部外者に漏洩する	・複雑で多数の設定条件と操作結果がわかりにくい脆弱性
		・攻撃者は、MFP へのジョブデータを一時蓄積するスプールサーバ内部に侵入し、スプールサーバ内に蓄積されるジョブデータを攻撃者にコピーして、ジョブデータに含まれる機密の情報を入手する	・他システム自体の脆弱性
2. 完全	・蓄積・外部処理サーバ(文書を蓄積するサーバやプロキシサーバ、コンテンツの変換処理などを行うサーバ)で文書またはアドレスが改ざんされる	・攻撃者は、蓄積・外部処理サーバと MFP の間の保護されていない通信に介入し、機密の情報を含むジョブデータを改ざんし、サポートセンタから顧客に新しいパスワードを送信させ、攻撃者が入手する	・他システムと MFP の通信が保護されていないか、保護が不完全である脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
性		・攻撃者は、MFP に対して蓄積・外部処理サーバになりすました偽の一時応答を返し、攻撃者が用意した偽の蓄積・外部処理サーバに MFP をリダイレクト接続させる	
		・スプールサーバ、またはスキャン結果を格納するファイルサーバ上で、ジョブデータまたはスキャン結果ファイルを、認証不要で書き換え可能な公開フォルダ上に格納していたため、攻撃者がすべて削除する	・機密の文書を書き換え可能なフォルダに置いてしまう人為的脆弱性
		・攻撃者は MFP に集中的にジョブデータを投入するスプールサーバの脆弱性を悪用してスプールサーバ内部に侵入し、機密の情報を含むジョブデータを改ざんする。	・他システム自体の脆弱性
3. 可用性	・MFP の停止または誤動作、乗っ取りにより、蓄積・外部処理サーバが停止するか誤動作する ・蓄積・外部処理のサーバが停止し、MFP の利用者が MFP を利用できなくなる	・攻撃者は MFP が蓄積・外部処理サーバと通信するポートに対しファジング試験を行い、特定の脆弱性に対して侵入するメッセージを作成し、一般のパソコンに感染させたマルウェアから特定の MFP に送信する。メッセージを受信した MFP は停止するか、誤動作を起こし、利用できなくなる	・MFP が蓄積・外部処理サーバと通信するポートに接続できるホストかサーバを特定し、制限していない脆弱性 ・MFP と蓄積・外部処理サーバとの間の通信を保護していない脆弱性
		・攻撃者は、MFP と蓄積・外部処理サーバとの間の特定のセッションに対して、「通信終了」または「メッセージ終了」などのメッセージをなりすまして挿入し、セッションを異常終了させる	・MFP と蓄積・外部処理サーバとの間で相互認証していない脆弱性 ・MFP の他システム用通信ポートで、予想外のデータを受信すると停止または誤動作する脆弱性
		・攻撃者が、負荷分散設定がある MFP に、負荷分散処理を許可した大量のジョブデータを投入し、負荷分散対象の MFP も含めて、複数台の MFP が同時に利用不能になる	・受付可能な処理要求量を見積もって、処理要求量を制限できない脆弱性 ・一度に投入できるジョブデータの上限を決めて、制限していない脆弱性
		・攻撃者は共有ファイルサーバの脆弱性を突いて、共有ファイルサーバを停止させ、共有ファイルサーバ経由でのファイル転送での MFP のスキャナ機能とファクスの配信機能が利用できなくなる	・蓄積・外部処理サーバ自体の脆弱性
4.	・偽の蓄積・外部処理サーバとの間で文書とアドレスを送受信してしまう	・攻撃者が動作させた偽の共有ファイルサーバに、電子ファイルを格納したため、機密の文書が攻撃者に漏洩する	・蓄積・外部処理サーバと MFP との間で相互認証を行っていない脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
真正性		・攻撃者が動作させた偽のメールサーバを経由してファクスメールが MFP に送られ、送信者を偽装した偽の請求ファクスが着信し、間違った口座に送金した	
5. 責任追跡性	・特定の蓄積・外部処理サーバが扱うデータが、どのサーバを経由して伝送されたものであるか、確認できない。不具合があっても原因を特定できない ・正しい経路で通信が行われているかどうか確認できない	・攻撃者が、あるメールサーバの脆弱性を利用して MFP に偽の配信要求を送信したが、MFP には記録がなく、どのメールサーバが攻撃に使われたか特定できず対策を立てられない	・電子メールの転送経路を含むメールヘッダは保護されていない脆弱性
		・MFP と蓄積・外部処理サーバとの間の通信について、多数の認証失敗の通信履歴が記録されていたが、通信相手のホスト名は DNS サーバ上で偽装されたもので、ホスト名から相手サーバを特定できなかった	・MFP 内部に記録する利用者端末との通信履歴の内容のうち、逆引きされたホスト名は DNS で偽装される脆弱性
6. 否認防止	・特定の蓄積・外部処理サーバの処理記録について、サーバを特定する情報が確かである根拠を示せない	・蓄積・外部処理サーバとの間の転送記録のうち、IP アドレスについては認証時に記録されるが、セッション情報を利用してほかの IP アドレスからもサービスを利用できるため、攻撃者は記録にない IP アドレスから攻撃を行う	・操作の記録に蓄積・外部処理サーバの IP アドレスが記録されていたが、その IP アドレスは利用者から任意の文字列を投入できる脆弱性
		・MFP と蓄積・外部処理サーバとの間の転送記録のデータは、SQL インジェクションで改ざんされていることがわかり、原因調査に使えない	・操作の記録に蓄積・外部処理サーバの IP アドレスが記録されていたが、その記録は第三者が改ざん可能な脆弱性
		・ファクスの中継機能を利用した多段の配信で、途中に不正なファクスが中継を行っていないことを確認しようとしたが、2 段目のメールファクスの一部で、どこからのファクス着信があったか通信記録の項目が欠けていたため、経路の確認ができなかった	・外部・蓄積システムとの間で通信を行った履歴が MFP に記録されていない脆弱性 ・外部・蓄積システムとの間で通信履歴に、充分な記録が含まれていない脆弱性
7. 信頼性	・蓄積・外部処理サーバから MFP が受信したジョブデータが壊れている ・MFP から蓄積・外部処理サーバに送信したジョブデータが正しく保存または処理されない	・攻撃者は、MFP に対して、特定の業務サーバになりすまして偽の応答メッセージを返す。偽の HTTP 応答メッセージには SQL インジェクションをしかけて、MFP 内部のデータベースを破壊する	・不十分な入力の検査、数値データによる脆弱性 ・MFP と蓄積・外部処理サーバとの間の通信が保護されていない脆弱性
		・MFP から特定の業務システムに対して、特定のデータ取得要求を送ると、失敗応答を返したり、タイムアウトを起こしたりするが、MFP 内部のソフトウェアは成功応答が返るまで処理を繰り返し、以後複数のプロセスが起動するためリソース不足に陥る	・競合、リソース管理が不十分な脆弱性

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性
		・攻撃者は MFP から負荷分散処理のために送信される、別の MFP への処理要求を、再びスプールサーバにリダイレクトさせて投入させ、ジョブデータを無限に循環処理させる	・すでに処理が済んでいるジョブデータを識別していない脆弱性 ・MFP と蓄積・外部処理サーバとの間の通信を保護していない脆弱性
		・外部のファイルサーバが脆弱性を突かれて侵入され、MFP から送信したファクスイメージやスキャンイメージのファイルが正しく保存されず、利用できない	・蓄積・外部処理サーバ自体の脆弱性

7.17.1 想定される被害の例

1) 継続的に、保護されているはずの機密の文書が漏洩するか、改ざんされる
2) 継続的にアドレス帳の一部が漏洩する
3) トナー、用紙などの消耗品を不要に消費する
4) MFP を利用できなくなる(一般利用者)

7.17.2 およそのCVSS 2.0 基本評価基準(一部)の影響度

1) AV:攻撃元区分　　ローカル～ネットワーク
2) AC:攻撃条件の複雑さ　高～中
3) Au:攻撃前の認証要否　複数～不要

8. 脆弱性の詳細解説

本章では、MFP に係わる代表的な脆弱性について、概要、解説、対策、その他参考情報について紹介する。

ここでは、MFP に独特な脆弱性で、一般的に知られていない可能性が高く見落としがちと考えられるものについて 6 件の脆弱性を選定している。

前半の 5 件の脆弱性については、MFPに独特な面がある。「9. ユニット間でデータを盗聴される問題」と「11. 複数配信を一括して実行する機能による問題」は、MFPが複数の機能を組み合わせて構成されるために持つ脆弱性である。

「10. ドライバ用プロトコルを経由した侵入の問題」と「12. 多数のプロトコルに含まれる脆弱性による問題」は、ドライバ用プロトコルと、その他サービスや監視、運用のためのプロトコルも含め、MFPをネットワーク上で利用するために多数の種類のプロトコルが実装されている問題に注目している。

「13. 遠隔保守インタフェースの悪用から起こる問題」については、MFPが組込み機器でありながら、その多機能性や消耗品の管理の必要性から、遠隔保守が必要とされる製品だというMFP独特な事情を反映している。

「14. 着脱式媒体を利用したMFPの構成変更による問題」では、多機能なMFPの膨大な設定項目を一括して設定し、多数のソフトウェアを間違いのないように一括して構成するために提供されている保守者向けの機能について、あまり知られていない問題として脆弱性の可能性を紹介している。

詳細解説では、参考情報として共通脆弱性評価システム「CVSS 2.0」を利用して、被害の影響度を数値で示している。評価値のうち、CVSS基本値について深刻度を 3 レベルに分ける基準についてはIPA「脆弱性の深刻度評価の新バージョンCVSS v2 について」[12]を参照いただきたい。

[12] IPA「脆弱性の深刻度評価の新バージョンCVSS v2 について」
http://www.ipa.go.jp/security/vuln/SeverityLevel2.html

9. ユニット間でデータを盗聴される問題

9.1 概要

MFP はプリンタ、スキャナ、ファクスなどの複数のユニットを組み合わせた製品である。これら複数のユニット間の通信が暗号化などで保護されておらず、攻撃者による MFP への物理的なアクセスが可能になると、ユニット間のインタフェース上で文書やアドレスの一次資産が盗聴される可能性がある。

9.2 解説

9.2.1 【攻撃手法とその影響】

スキャンユニットと実行基盤の間や、ファクスユニットと実行基盤の間など、ユニット間の通信バスが USB などの標準インタフェースで接続されている場合、標準的な USB モニタや USB アナライザを利用して、USB バス上の通信データを取り出すことができる。

下の図 9-1は、MFP内部のスキャンユニットと実行基盤の間がUSBバスで接続されていた場合、USBモニタを挿入してユニット間の通信データを盗聴する構成図である。スキャンユニットと実行基盤は本来であれば図 9-1の下の点線のように直接、接続される配線があるが、攻撃者はUSBケーブルの配線を変更して、USBハブを間に挿入し、USBモニタを接続する。

USB モニタでは、同じ USB ハブ上を経由して伝送される通信データを常時監視し、スキャンユニットと実行基盤の間の通信データを盗聴できる。

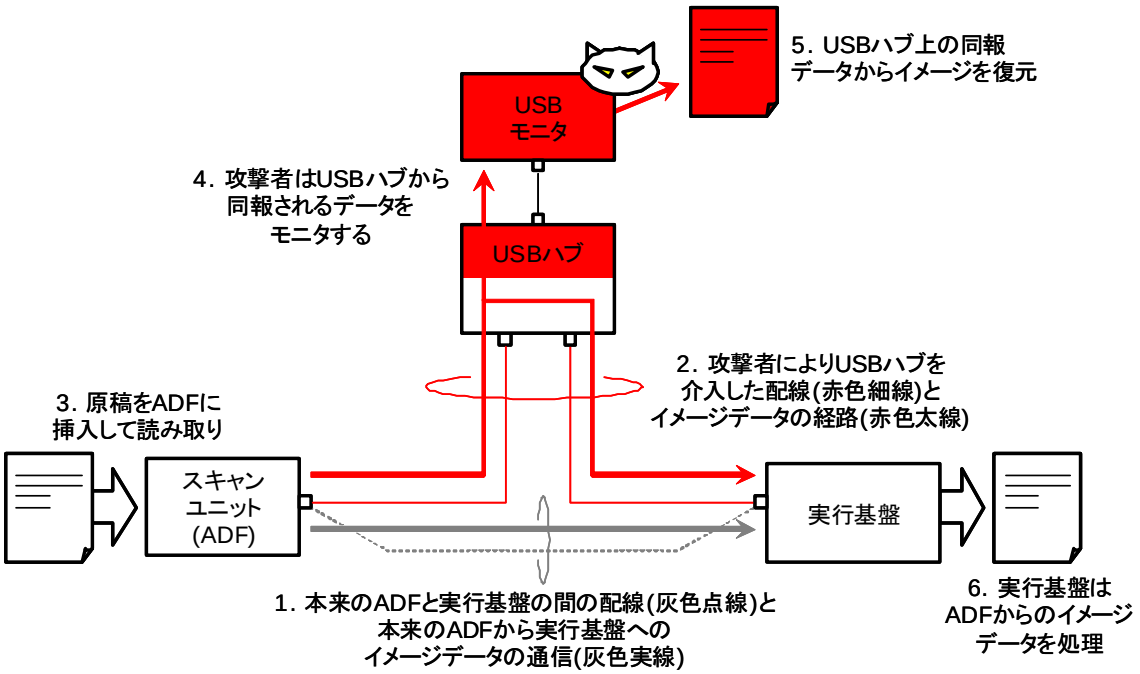

図 9-1 スキャンユニットと実行基盤の間に USB モニタを挿入した図

この攻撃手法はまず、ユニット間のバス配線が標準的なインタフェースで構成

されている前提が必要になる。また、実行するには MFP 本体へのアクセスが必要で、さらに MFP 本体の実行基盤ユニットを引き出すか、スキャンユニットも引き出して配線を変更する必要があるだろう。また、MFP 本体のユニットの取り出し作業には、一部の手順や工具にメーカ独自のものがあると見られ、一般的には安全な作業を行うにはメーカの保守者や保守業者相当の知識と経験が必要だと考えられる。

こうしたことから、上記の例に限っては実現される影響は非常に少ないと考えられる。ただし、MFP 内部の標準インタフェースは USB だけに留まらないところに問題があると考えられる。

なお、本事例についての具体的な攻撃事例は見当たらなかったため、脆弱性情報の信頼性としては「未確認の情報源のみ」としている。

9.2.2 【原因と考察】

下の図 9-2はMFP内部での複数のユニットまたはモジュールのハードウェア的な接続の例である。MFPでは、プリント、スキャン、ファクス、コピーなどの複数の機能を一体にした機器だが、それぞれの機能をユニットやモジュールとして、組み立てやすいように別の装置として準備し、組み立てる構成になっている。

複数のユニットやモジュールはそれぞれ、通信を行うために専用の通信ケーブルか、標準化された通信手順を利用する標準ケーブルで接続される。専用の通信ケーブルの場合、その詳細な技術仕様を調べる障壁があるため、ケーブル上での盗聴の難易度は高い。しかし、標準的な手順を利用した標準ケーブルであれば、通信中のデータをすべて取り出して確認するための「モニタ」や「アナライザ」などの装置が利用できる。

また、MFP が本体内部で利用しているインタフェースのうち、ハードディスク用のインタフェース以外では、ケーブルやカード用のスロット上で通信データの暗号化など、通信データの保護を行っている部分はほとんどないと考えられる。

こうした標準インタフェース用のモニタ機器は一般に製品開発に利用するため、機材自体が大きく、MFP に組み込んで内蔵させることはまだ難しいと考えられる。しかし、USB 3.0 や SATA などの将来的に MFP にも普及の可能性がある高速インタフェースについては、さらに手順や電気的条件が共通化される方向にあるため、ユニット間の接続をモニタするための技術的な障壁は低くなりつつあると考えられる。

本書の執筆現在では、MFPではすでにハードディスクユニットへの通信が暗号化されている。追加のハードディスク暗号化モジュールや暗号化処理ソフトウェアなどにより、ハードディスクと実行基盤の間のデータが暗号化されるのが一般的である。また、ICカード認証装置と実行基盤の間の通信手順はFeliCaやeLWISEなどのように安全性を備えた手順が用意されている。図 9-2の実行基盤の右下、パラレルインタフェースと、USBプリント機能については、ネットワーク上でMFPを共有する場合は一般的には不要と考えられるため、インタフェースそのものを無効にして利用するだろう。その一方、USBポートをTCP/IPで中継してUSBケーブルをTCP/IPで延長するような利用方法もある。この場合はUSBプリント機能や着脱メディアなども延長できる場合があり、通信データの保護に注意が必要である。

なお、各ユニットまたはモジュール間のインタフェースについては「3.8.7 MFP 内部のハードウェア – モジュール間の接続」に紹介しているので参考にされたい。

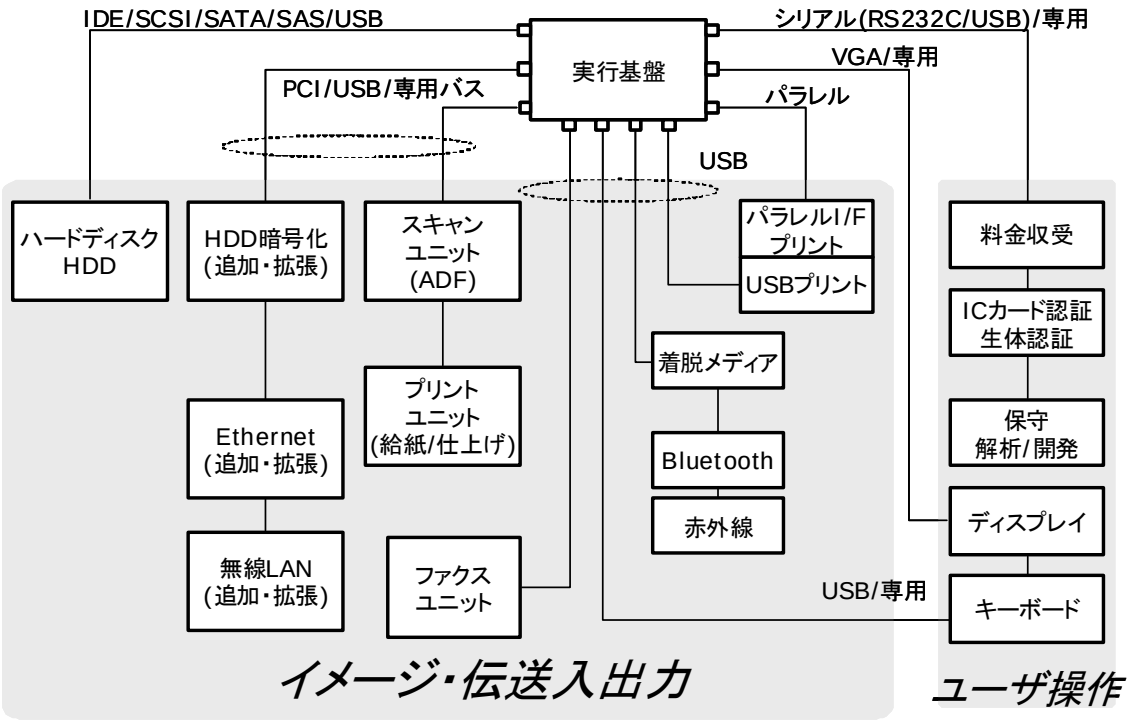

図 9-2 MFP 内部のユニットまたはモジュールの接続構成例

9.3　対策

9.3.1　【運用ガイド】

1) MFP 本体を設置した部屋は入退室管理を行い、許可された人だけが入室できるようにする
2) MFP 本体に不要な機器や装置が付着または装着されていないことを確認する
3) MFP 本体の保守作業には立会う
4) MFP 製品のセキュリティガイドを参照し、メーカに質問し、理解に努める。

9.3.2　【実装ガイド】

1) MFP 本体内部へのアクセス難易度を高める
2) 高速大容量の標準通信バスには通信データ保護機能の搭載を検討する
3) USB を TCP/IP で延長する際のセキュリティガイドを取扱説明書に明記する

9.4　参考情報

公開年月	情報源
2002 年 10 月	USB Sniffer http://sourceforge.net/projects/usbsnoop/ USB インターフェース上のデータをモニタするオープンソースソフトの例。その他製品多数。

2005 年 5 月	サイレックス・テクノロジー、USB デバイスサーバ SX-2000U2 新発売 http://www.atpress.ne.jp/view/2877 複数の MFP メーカが Silex Technology 社の USB デバイスサーバをオプション品として採用している。
2009 年 7 月	USB/IP Project http://usbip.sourceforge.net/ USB デバイスを IP ネットワーク上で共有できるようにするオープンソースプロジェクト。
2009 年 8 月	Defcon 17 - USB Attacks: Fun with Plug and 0wn http://www.defcon.org/images/defcon-17/dc-17-presentations/defcon-17-rafael_vega-usb_attacks.pdf USB プロトコルの概要と、IP 上で転送させてファジングを行う概要までを紹介。

9.5　CVSS深刻度評価(参考値)

スキャナと実行基盤の間が USB で接続されている場合に、USB で伝送されるイメージデータが USB モニタを利用して盗聴できるという脆弱性について、CVSS 2.0 で深刻度を評価した。

9.5.1　【評価結果】

本脆弱性の深刻度	□Ⅰ（注意）	■Ⅱ（警告）	□Ⅲ（危険）
本脆弱性の CVSS 基本値		4.6	
本脆弱性の CVSS 現状値	3.4		

9.5.2　【CVSS基本値の評価内容】

攻撃元区分	■ローカル	□ 隣接	□ネットワーク
攻撃条件の複雑さ	□高	□中	■低
攻撃前の認証要否	□複数	□単一	■不要
機密性への影響	□なし	■部分的	□全面的
完全性への影響	□なし	■部分的	□全面的
可用性への影響	□なし	■部分的	□全面的

9.5.3　【CVSS現状値の評価内容】

攻撃される可能性	□未実証	■実証可能	□攻撃可能	□容易に攻撃	□未評価
利用可能な対策のレベル	■正式	□暫定	□非公式	□なし	□未評価
脆弱性情報の信頼性	□未確認	■未確証	□確認済み		□未評価

10. ドライバ用プロトコルを経由した侵入の問題

10.1 概要

クライアントから MFP を操作するドライバプロトコルの脆弱性により MFP の制御システムが侵入される。ここではドライバプロトコルとして LPR の例をとりあげる。

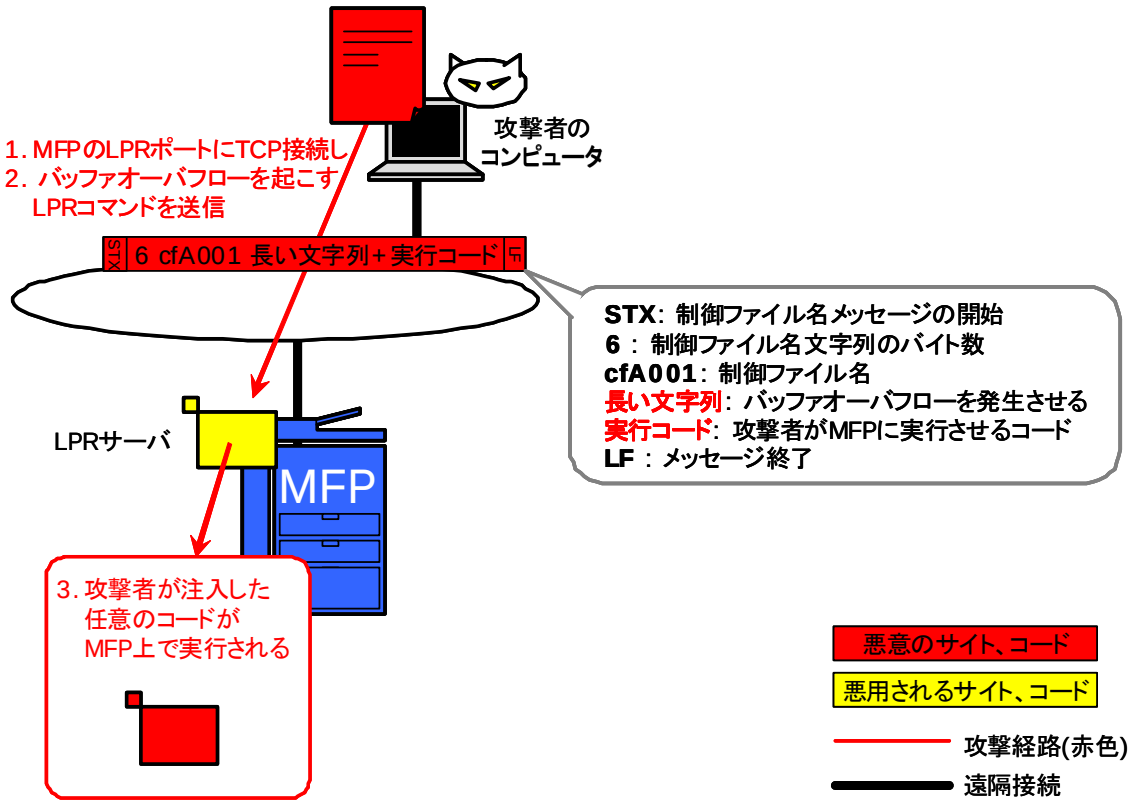

図 10-1 ドライバ用プロトコル LPR を経由した侵入の例

10.2 解説

10.2.1 【攻撃手法とその影響】

はじめに攻撃者は MFP 上で実行されている LPR サーバの TCP ポート 515 番に TCP 接続する。LPR プロトコルにはユーザ認証の手順はないため、攻撃者は MFP 上の LPR サーバに対して無条件で LPR コマンドを送信できる。

攻撃者は MFP 上の LPR サーバに対して、プリント用の制御ファイルのファイル名として、予想外の長い文字列を与えてバッファオーバフローを起こさせる。この非常に長い文字列に続けて、攻撃者は任意の実行コードを LPR サーバに送り最後に LPR のコマンド終端文字として改行コード(LF: 0x0a)を送ると、LPR サーバ内でバッファオーバフローが発生し、攻撃者が送り込んだ実行コードに制御が移る。下の図 10-2に、LPRコマンドによる侵入のシーケンス例を示す。

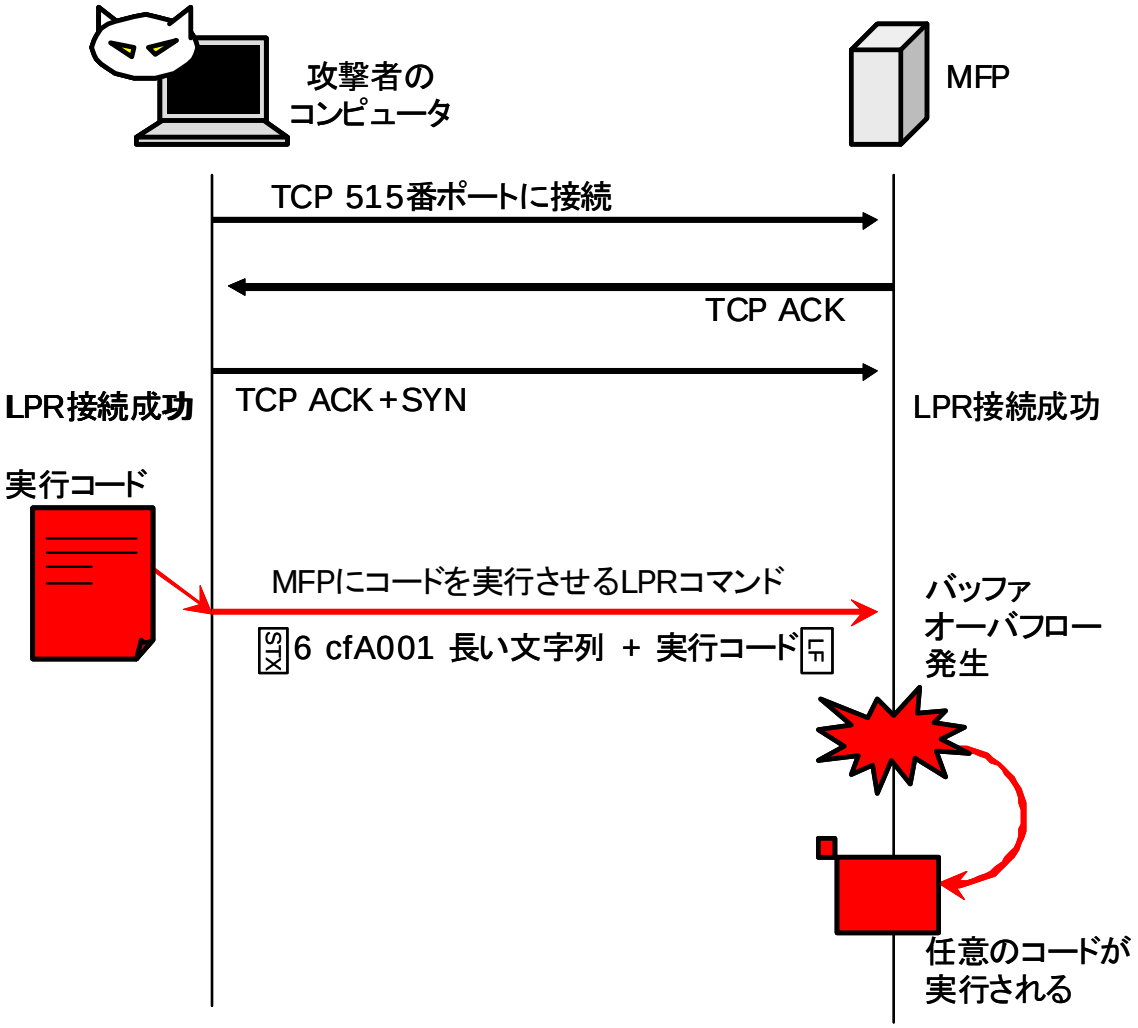

図 10-2 ドライバ用プロトコル LPR コマンドによる侵入のシーケンス例

その結果、MFP 上の LPR サーバを実行している実行環境で、攻撃者による任意のコードが実行させられる。攻撃者が MFP 上で任意のコードを実行できると、MFP 上でさらに別のプログラムを導入して実行させたり、MFP が扱う文書やジョブデータを攻撃者のホストにコピーしたり、MFP から別のホストへの攻撃が可能になる場合がある。また、攻撃者が MFP 上で任意のコードを実行できなかった場合でも、MFP 上の LPR サーバ内でバッファオーバフローが発生すると、その LPR サーバなどの動作が停止するか、LPR サーバまたは MFP 全体が再起動することがあり、結果としてその MFP の LPR サーバか、MFP 全体が一時的に利用できなくなる。

10.2.2 【原因と考察】

LPR プロトコルでは、印刷を制御するためにいくつかのコマンドが標準化されている。しかし LPR プロトコルのコマンドでは引数となる文字列は LF(Line Feed) コードで区切られているだけでコマンド文字列の長さを示す引数がない。また、

転送されるジョブ制御ファイルとジョブデータファイルのファイル名を指定するコマンドがあるが、ファイル名には任意の文字列を指定でき、ファイル名の文字列長を指定する引数がない。また、制御ファイル、ジョブデータファイルともに、転送するファイルの長さをバイト単位で示す引数があるが、テキスト形式による数字での指定となっており、ファイルの長さを示す数字の表現には桁数や最大長に制限がない。

LPR プロトコル仕様を標準化した RFC 1179 では、ジョブ制御ファイル名とジョブデータファイル名の文字列長は 6 文字程度になる仕様になっているが、LPR プロトコル上では文字列長の制限はないため、何文字でも送り込むことができる。

また、テキストで表現された数値の扱いで、予想外の範囲を指定されてヒープメモリのオーバランが発生することもありえる。

このようなテキスト表現による「リラックスした」プロトコル仕様は HTTP や SMTP、SIP のような手順に共通しているが、逆に言えば厳密な形式ではなく自由度が高い分、受信する側での詳細な検査が必要になる。このような、外界から受信したデータの検査処理は「入力値の確認」や「入力データの無害化」、「サニタイジング」などと呼ばれる。IPA ではこの脆弱性と開発上の対策について「セキュア･プログラミング講座」”C/C++言語編・著名な脆弱性対策”で、イメージ図入りの解説をウェブで公開しているので参考にしていただきたい。

この攻撃が成功しやすい前提条件として、注入した実行コードを攻撃者の意図通りに動作させるため、MFP 上の LPR サーバ実行環境が Linux や Windows、VxWorks などのよく知られた OS で、利用されている CPU またはマシン語もよく知られたものである必要がある。また、スタックメモリ上やヒープメモリ上に配置したマシン語を実行できる環境が必要である。

この例では、MFP を利用できるネットワークからの攻撃であるため、一般的には攻撃者のパソコンは排除されているはずである。しかし、利用者のパソコンがウイルスやマルウェアに感染したり、一部の許可されていないコンピュータがネットワーク内に接続されてしまったりした場合は、MFP のドライバプロトコルの脆弱性を狙った攻撃がありえる。

なお、MFPのドライバプロトコルは多数のプロトコルがサポートされており、LPRのような脆弱性はその他のドライバプロトコルにも残存している可能性がある。MFP製品の開発者は、下の表 10-1に示したようなMFPで利用されるドライバプロトコルのそれぞれについて、脆弱性の確認が必要である。一方、MFPの利用者がセキュリティの確保をするときは、MFP製品ごとに必要な脆弱性対策を実施して、必要な利用条件を守る必要がある。

表 10-1 MFP で利用されている主なドライバプロトコル

ドライバプロトコル	用途	認証手順の有無	暗号化手順の有無
LPR	プリント	-	-
RAW9100	プリント	-	-
IPP	プリント	○	○
SMB	プリント、スキャン	○	○
TWAIN	スキャン	○	○
FTP	スキャン	○	○
WebDAV	スキャン	○	○
SMTP	ファクス	○	○

POP3	ファクス	○	○
IMAP4	ファクス	○	○
WSD (Web Service Discovery)	プリント、スキャン、ファクス	○	○
BMLinkS	プリント、スキャン、ファクス	○	○

10.3 対策

10.3.1 【運用ガイド】

1) LPR, RAW9100, IPP, SMB, WS/Print, SOAP, WebDAV など、MFP 上で利用するサーバを特定し、MFP 上で利用しないサーバ機能と、サービスの待ち受けポートを停止しておく
その上で、MFP メーカの脆弱性情報を確認し、必要な対策があれば実施を検討する
2) MFP に対してジョブデータを投入できるホストとして、特定のプリントスプールサーバや、スキャンとファクスのゲートウェイサーバなどに限定する
3) MFP 上でドライバプロトコルを受け付ける利用者端末の範囲を IP ネットワーク単位で制限する
4) 相互認証方式を持つドライバプロトコルと、ドライバソフトウェアを利用し、正しく運用する

10.3.2 【実装ガイド】

1) MFP の運用セキュリティが必要な環境ではどのような運用が適切か取扱説明書に記述する
- MFP 上で、どのプリントサーバを動作させるのが適切か
- どのプリンタドライバをどのように設定するのが適切か
- プリントスプーラの利用方法
- MFP をどのようにネットワーク上で隔離するか、など
2) MFP 製品のサーバソフトウェアでの入力検査を行い、脆弱性試験を行う
3) MFP 上で実行されるサーバが受け入れを許可、または禁止する IP アドレスの範囲を指定できるようにする

10.4 参考情報

公開年月	情報源
1990 年 8 月	RFC 1179 Line Printer Daemon Protocol http://tools.ietf.org/html/rfc1179 IETF による LPR のプロトコル仕様。
1998 年 7 月	LPRとはなんですか? http://support.apple.com/kb/TA21876?viewlocale=ja_JP&locale=ja_JP アップルコンピュータのサポート情報より。PAP(Apple社のAppleTalk上で利用できるプリントジョブ伝送手順"Printer Access Protocol"とLPRとの違いが説明されている。
2000 年 10 月	LPD Vulnerability Issues http://lpd.brooksnet.com/lpd-security.html 次のような指摘と、プリントサーバ側での対策例を示している。

	(1)LPR 経由でプリントサーバ上に任意のファイルを作成できる (2)LPR 経由でプリントサーバ上の任意のファイルを削除できる (3)LPR 経由でプリントサーバ上の任意のコマンドを実行できる
2001 年11月	CERT® Advisory CA-2001-30 Multiple Vulnerabilities in lpd http://www.cert.org/advisories/CA-2001-30.html LPR のプリントサーバ側(lpd)の複数の脆弱性。 (1)バッファオーバフローにより任意のコードが実行させられる (2)プリントサーバ上で sendmail に任意のオプションを指定できる
2006 年 10 月	LPR プロトコルと標準 TCP/IP ポート・モニタの違い http://www.atmarkit.co.jp/fwin2k/win2ktips/809stdprnprt/stdprnprt.html Microsoft 社の TCP/IP ポート・モニタで使われる RAW9100 と LPR の違いが説明されている。
2007 年 10 月	US-Cert: Cisco IOS LPD buffer overflow vulnerability: VU#230505 https://www.kb.cert.org/vuls/id/230505 Cisco IOS の LPD で、99 文字を超えるホスト名を入力すると sprintf()の呼出し後にバッファオーバフローが発生する。
2010 年 4 月	Mocha W32 LPD Remote Buffer Overflow Vulnerability http://www.securityfocus.com/bid/39498/info Mocha 社の Windows 用 LPR プリントサーバソフト上で、LPR の制御ファイル受信コマンドで制御ファイル名文字列のバッファオーバフローにより任意のコードが実行される脆弱性。Python スクリプトによる手順の実証コードがある。

10.5 CVSS深刻度評価(参考値)

LPR サーバで任意のコードが実行される脆弱性について CVSS 2.0 で深刻度を評価した。

10.5.1 【評価結果】

本脆弱性の深刻度	□ Ⅰ（注意）	□ Ⅱ（警告）	■Ⅲ（危険）
本脆弱性の CVSS 基本値			7.5
本脆弱性の CVSS 現状値		5.9	

10.5.2 【CVSS基本値の評価内容】

攻撃元区分	□ローカル	□ 隣接	■ネットワーク
攻撃条件の複雑さ	□高	□中	■低
攻撃前の認証要否	□複数	□単一	■不要
機密性への影響	□なし	■部分的	□全面的
完全性への影響	□なし	■部分的	□全面的
可用性への影響	□なし	■部分的	□全面的

10.5.3 【CVSS現状値の評価内容】

攻撃される可能性	□未実証	■実証可能	□攻撃可能	□容易に攻撃	□未評価
利用可能な対策のレベル	■正式	□暫定	□非公式	□なし	□未評価
脆弱性情報の信頼性	□未確認	□未確証	■確認済み		□未評価

11. 複数配信を一括して実行する機能による問題

11.1 概要

MFP ではスキャンしたイメージやファクスで受信したイメージを複数の宛先に一括して送信する機能がある。このとき、一括して送信する複数の宛先の中に意図していない宛先が含まれていると、機密の文書が漏洩する。

11.2 解説

11.2.1 【攻撃手法とその影響】

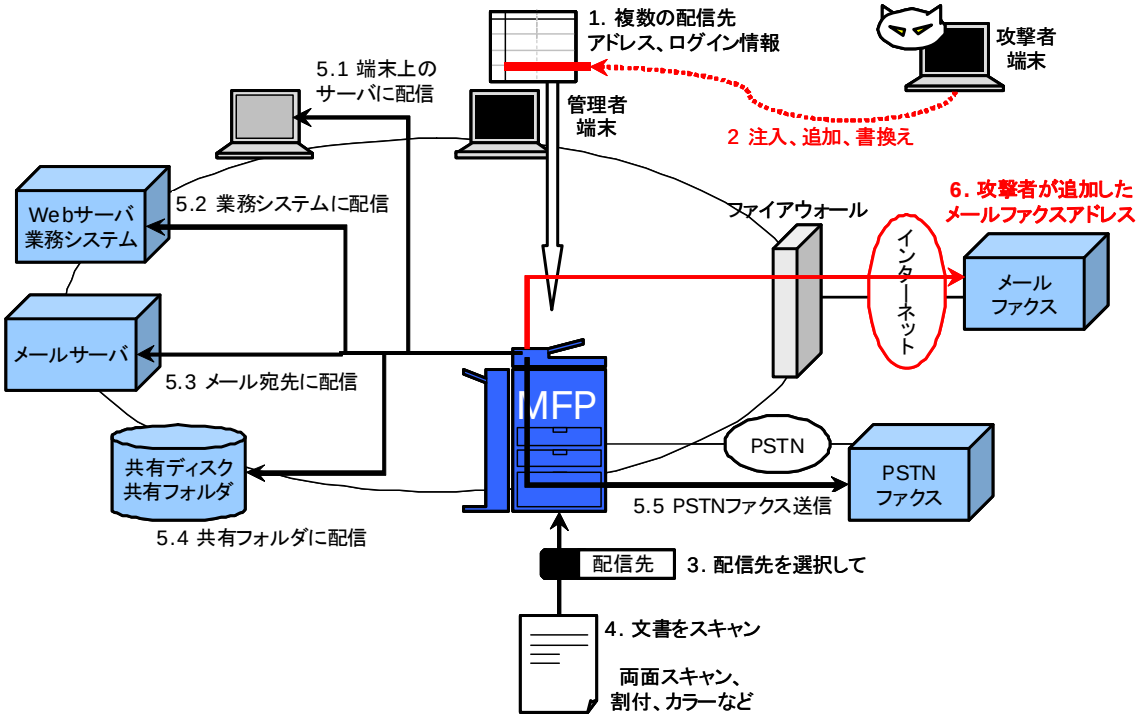

図 11-1 複数配信を一括して実行する例

上の図 11-1は、ある文書を所定の手順でスキャンして、スキャンしたイメージを複数の配信先に一括して配信、転送する処理の例と、攻撃例を示したものである。

この例ではまず、図 11-1の中央上で管理者端末から複数の配信先のアドレスとログイン情報などを一括してMFPに投入する。この手順の前後で、攻撃者端末は管理者端末になりすましたり、管理者端末にリクエスト強要攻撃を実行したりして、攻撃者のメールファクスアドレスを追加する。

次に MFP の利用者が MFP のコンソールでこの配信先を選択し、所定の文書をスキャン台に置き、MFP のスタートボタンを押すと、所定のスキャン方法で文書がスキャンされ、自動的に複数の配信先に文書イメージが転送される。

この中のひとつのアドレスに攻撃者のアドレスが紛れ込んでいる場合、利用者は特に知らないまま、攻撃者にも機密の情報を転送してしまう。

MFP の管理者は、定期的に正常に配信処理された記録を確認するか、一括配信設定を確認しないかぎり、意図しない宛先への配信を検出できない。また、この攻撃はインターネット上のメールサーバやメールファクスなど、インターネット上のサーバを経由する場合、どこからどこへと文書が転送されたか、追跡しにくくなる。

このような攻撃は一般には管理者端末の操作権限が必要なため、かならずしも容易ではないものの、管理者の端末がリクエスト強要攻撃などで攻撃者に操られてしまうと現実のものになる。

11.2.2 【原因と考察】

複数の配信先への一括送信の問題としては、不正な宛先が紛れ込むことの問題と、個々の送信処理の結果がわかりにくい点にある。不正な宛先が紛れ込む件は上記の攻撃例で紹介した。個々の送信処理の結果については、メールサーバへの配信は相手のメールボックスの空き容量がなくなったり、PSTN ファクスへの送信は相手ファクスが通話中のために配信できなかったりする、などの失敗が考えられる。複数宛先への配信処理の一部の失敗については、ジョブ名や宛先名の表示方法も含めて、MFP がどのような表示または通知を行うかによってわかりやすさが大きく異なるだろう。

MFP では文書をサーバや端末、その他 MFP などの他システムに送信する方法が複数提供されている。これら送信は大きく分けてファクス、メール、サーバに分かれる。それぞれの特徴と、関連する脆弱性を紹介する。

複数の配信先への一括配信は、ファクス受信時の親展ボックス名や発信/着信ファクス ID などを起点にする場合と、スキャン処理を起点にする場合があるため、この二つについて説明する。

1)　ファクス(PSTNファクス、ファクス網ファクス、メールファクス、SIPファクス)

原稿を光学読み取りするか、利用者端末からファクス送信ドライバソフトウェアなどを利用してイメージデータを送信する。宛先では、通常はファクス受信機で受信する。

PSTN ファクスでは、個別に宛先のファクスの電話番号を指定でき、宛先が PSTN ファクスであればどこにでも送信できる。そのため一般利用者が宛先を間違って入力してしまうか、複数配信先のアドレスの一部アドレスが改ざんされるだけで、攻撃者にも機密の文書が配信される可能性がある。

ファクス網を利用した「ファクス網ファクス」は、ファクスの同報に特化したサービス網を利用し、配信先の管理はファクス網提供事業者が行うため、一般利用者が個別に宛先を入力して同報送信することがなく、比較的安全である。しかし、PSTN 網をベースにしており低速なため相対的に運用費用が高い。

メールファクスはインターネット上でも利用できるメールを伝送媒体としたファクスである。ITU-T T.37[13]として標準化されている。高速で、パソコン間でも送受信できる柔軟性がある。S/MIMEを利用してファクスイメージの暗号化や電子署名による保護ができる。S/MIMEを利用する場合は宛先の電子証明書をMFPから利用できるようにしておく必要があり、許可されていない宛先用の電子証明書がMFPに提供されると、攻撃者に機密の文書を暗号化され送信されてしまうことがある。また、メールファクスには途中の転送経路にメールサーバを利用する方法

[13] ITU-T.37 – Procedures for the transfer of facsimile data via store-and-forward on the Internet - http://www.itu.int/rec/T-REC-T.37/en

と、MFPから直接相手のMFPにSMTP接続する方式がある。機密の文書の重要度が高い場合で、メールサーバを利用するときには、途中に介入するメールサーバが信頼できるサーバかどうか、確認する必要があるだろう。一方、宛先MFPへのSMTPでの直接転送を行う場合、ファイアウォールなどの障壁のために接続できないことがある。

SIPファクスは、PSTN公衆網をIP化した、SIPというプロトコルを利用してファクスイメージを転送する方式である。ITU-T T.38[14]として標準化されている。SIPファクスには、MFP本体がSIPに対応した場合と、既存のPSTNファクスにSIP TA(Terminal Adapter)を装着してSIPファクスを利用する方法がある。

SIPファクスでは、一般的にSIP通信の保護が行われていない。一部でDTLS(RFC 4347)[15]やZRTP[16]などの保護機能を利用したSIP製品も提供されているが、まだ一般的ではない。そのため、SIPファクスをインターネット経由で利用することは危険である。SIPファクスをインターネットや、保護されていない無線LANなどで利用すると、盗聴や宛先の改ざん、第三者による介入を容易に許すことになる。そのため、機密の文書の重要度が高い場合、SIPファクスを利用するときには、通信事業者のSIP向けの閉域通信サービスを利用するか、自営のVPN網の利用を選択することになるだろう。ただし、機密の文書の重要度や頻度が極めて低い場合は、コスト優先でインターネットを経由して利用することも選択できるだろう。

SIPに関する脆弱性についてさらに知りたい方は「SIPに係る既知の脆弱性に関する調査報告書 改訂第 2 版[17]」を参照いただきたい。

2)　スキャン to X(ファクス、メール、サーバ、プリント)

スキャンしたイメージを特定のメールアドレスに送信したり、特定のサーバに送信して、ファイルとして格納したり、特定の処理や加工を行う。また、ファクスと同じように送信するか、紙にプリントすることもできる。

ファクスについては「1) ファクス(PSTNファクス、ファクス網ファクス、メールファクス、SIPファクス)」で詳しく紹介した。メールでの配信については、やはりファクスの配信方法の「メールファクス」で紹介したような方法とほぼ同じである。

サーバへの配信については、大きく分けて二つあり、ひとつは遠隔のファイルサーバなどにファイルとして格納するものと、OCR (Optical Character Recognition: 光学文字認識)などの自動文字読み取りやデータベースに格納するなどの特定の処理を行うものがある。

ファイルとして格納する手順については、SMB、FTP、WebDAV などの標準的な手順があり、MFP の利用環境の管理者が設定すれば利用できる。特にファイルとして格納するときの宛先はサーバが動作していればよいため、共有のファイルサーバのほかに、一般利用者の端末上のファイル共有機能でもよい。そのため、攻撃者が一般利用者の端末になりすましたり、任意の端末を用意したりしてファイルサーバの宛先として複数配信先に追加すると、攻撃者に機密の文書のコピーが転送されることになる。

特定の処理を行う Web サーバなどの他システムの場合は、そのサーバの URL を

---

14 ITU-T T.38 - Procedures for real-time Group 3 facsimile communication over IP networks - http://www.itu.int/rec/T-REC-T.38/e

15 RFC 4347 - DTLS: Datagram Transport Layer Security - http://tools.ietf.org/html/rfc4347

16 ZRTP - ZRTP仕様 - http://zfoneproject.com/zrtp_ietf.html

17 IPA「SIPに係る既知の脆弱性に関する調査報告書 改訂第 2 版」2009 年 4 月 http://www.ipa.go.jp/security/vuln/vuln_SIP.html

指定するか、特別な変換用のサーバの URL を指定することがある。これら他システムについては個別の処理は異なるが、HTTP をベースにした手順が多いため、攻撃者による不正なアドレスの追加だけではなく、これら他システム上での Web アプリケーションの脆弱性も脅威の対象となるだろう。Web アプリケーションの脆弱性について詳しく知りたい方は「安全なウェブサイトの作り方」を参照いただきたい。

11.3 対策

11.3.1 【運用ガイド】

1) イメージを非常に多数の拠点に配信する場合はファクス専用網(F-NET)や VPN などの閉じたネットワーク内でメールファクスや IP ファクスを運用する
2) 複数配信先の設定者、設定手順を決めておき、遠隔管理機能を安全に利用する
3) MFP 内部の配信先設定の変更履歴の記録から、複数配信設定の変更を監視し、複数配信先の構成状況を定期的に検査する
4) 許可されていない宛先の電子証明書が MFP 内のアドレス帳や共有アドレス帳に追加、混入していないか定期的に検査する
5) 配信先と配信ごとの成否を記録し、定期的に検査する

11.3.2 【実装ガイド】

1) 複数配信先を設定するユーティリティと MFP の間の通信路の保護
2) 不正アドレスの混入の自動検出機能

11.4 参考情報

公開年月	情報源
1998 年 6 月	ITU-T T.37 http://www.itu.int/rec/T-REC-T.37/en インターネット電子メールを利用したファクス伝送手順
2007 年 4 月	ITU-T T.38 http://www.itu.int/rec/T-REC-T.38/e SIP を利用したファクス伝送手順
2009 年 4 月	SIP に係る既知の脆弱性に関する調査報告書 改訂第 2 版 http://www.ipa.go.jp/security/vuln/vuln_SIP.html SIP/RTP に関する脆弱性と対策
2010 年 3 月	IPA 安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/websecurity.html Web サイトによくある脆弱性と対策、SQL インジェクション対策など

11.5 CVSS深刻度評価(参考値)

複数の宛先に異なる方式で文書を送信したとき、そのうちの一部に攻撃者のアドレスが含まれており、機密の文書がスキャンイメージの転送または配信として漏洩するときの影響を CVSS 2.0 で評価した。

11.5.1 【評価結果】

本脆弱性の深刻度	■Ⅰ（注意）	□Ⅱ（警告）	□Ⅲ（危険）
本脆弱性の CVSS 基本値	3.5		
本脆弱性の CVSS 現状値	3.0		

11.5.2 【CVSS基本値の評価内容】

攻撃元区分	■ローカル	□隣接	□ネットワーク
攻撃条件の複雑さ	■高	□中	□低
攻撃前の認証要否	□複数	■単一	□不要
機密性への影響	□なし	■部分的	全面的
完全性への影響	□なし	■部分的	□全面的
可用性への影響	□なし	■部分的	□全面的

11.5.3 【CVSS現状値の評価内容】

攻撃される可能性	□未実証	□実証可能	□攻撃可能	□容易に攻撃	■未評価
利用可能な対策のレベル	□正式	□暫定	■非公式	□なし	□未評価
脆弱性情報の信頼性	■未確認	□未確証	□確認済み		□未評価

12. 多数のプロトコルに含まれる脆弱性による問題

12.1 概要

MFP は組込み機器の中でも最も多数のプロトコルを同時に実装し稼動させるシステムのひとつであると考えられる。このような多数の別々のプロトコルを一度に実装するため、どこかにわずかずつ含まれる脆弱性が順に発見され、攻撃に悪用される可能性がある。

12.2 解説

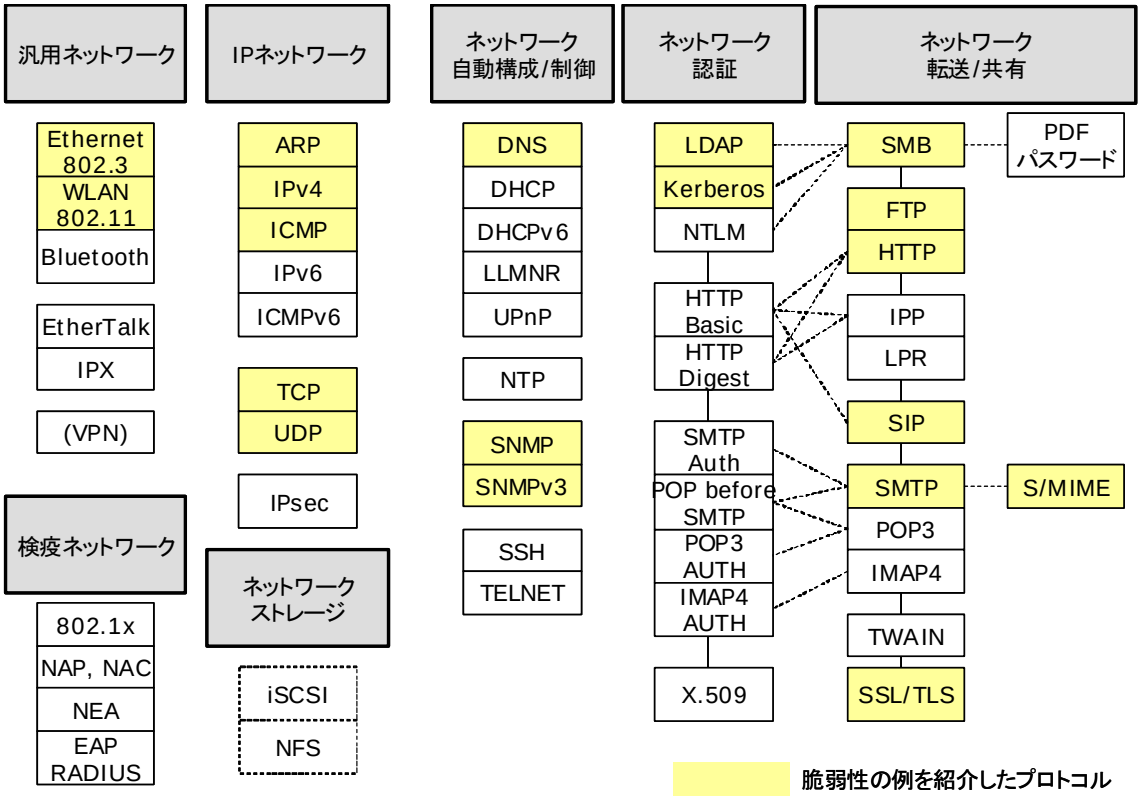

図 12-1 MFP で一般的に利用される通信プロトコルの一覧

上の図 12-1は、MFPで一般的に利用される通信プロトコルの一覧である。左上の「汎用ネットワーク」はEthernetや無線LANなどの物理的な通信プロトコルである。「検疫ネットワーク」は、MFPのような重要なホストを独立したネットワークに隔離し、重要なソフトウェアの更新が済んでいない端末をネットワーク上で自動的に隔離しておくことなどに利用される。「IPネットワーク」はインターネットを支えるための、複数のネットワークを相互接続し、HTTPなどのアプリケーションプロトコルを伝送する手順である。「ネットワークストレージ」はネットワーク上のハードディスクなどの格納装置を扱う手順だが、現在の主要MFPには該当がない。「ネットワーク自動構成/制御」は、IPアドレスを自動的に配布したり、ホスト名をIPアドレスに変換したり、サービス名をほかのマシンに広報する手順である。

「ネットワーク認証」は、MFPにネットワーク経由で接続する利用者端末や管理者の端末がMFPとの間で利用者名や識別IDを確かめ合う手順である。「ネットワーク転送/共有」は、MFPを介して文書データの交換や格納を行うための手順である。図 12-1の右半分にある点線で示している部分は、転送プロトコルと、それに対応または関連する認証プロトコルの関係を示している。例えばSMBというファイル共有プロトコルはLDAP、Kerberos、NTLMを認証プロトコルとして利用する。HTTPの場合は、HTTP Basic認証、HTTP Digest認証を利用する。IPPはHTTPベースであるので、同様の認証プロトコルを利用する。SIPはHTTPと似たような形式のプロトコルで、HTTP Basic認証と同じ手順を利用する。メールを転送するSMTPについてはSMTP AUTHとPOP before SMTPという認証手順がある。メールボックスにアクセスする手順のPOP3には、POP3 専用の認証プロトコル(POP3 AUTH)があるが、POP before SMTPはこれを利用している。メールボックスにアクセスする手順で、より高機能なIMAP4 にはIMAP4 専用の認証プロトコル(IMAP4 AUTHENTICATION)がある。
図 12-1の右上のPDFパスワードは、PDF型式のファイルにパスワードをつけて暗号化する機能である。これは通信プロトコルではないが、MFPの利用者が利用できるコンテンツの保護機能の一つである。また図 12-1の右側中ほどのS/MIMEも、メールのコンテンツを保護する機能で、メールの本文部分にあたるイメージデータを暗号化したり、電子署名を追加してイメージデータの改ざんを検出したりする機能がある。

上記のそれぞれのカテゴリごとに、複数のプロトコルが存在している。それにより、利用者は自分の環境に合ったプロトコルを選択して利用することができる。

例えば、「ネットワーク転送/共有」では、ファイル転送のプロトコルとして、SMB を使った SMB サーバへの書き込み、読み出しがある。FTP も FTP サーバへの書き込み、読み出しの手順となる。HTTP については HTTP プロトコル上でさらに拡張された、IP や SOAP を使った Web サービスも提供され、書き込み、読み出しのほかに、どのようなサービスがあるか広報する機能も提供されている。

一方、ファクスの送受信については、PSTN 公衆網を利用した、アナログファクスモデムによる伝送から、メールを伝送媒体に使った S/MIME 形式のファクス転送プロトコルと、SIP を使った SIP-FAX 手順がある。SIP の場合には、NGN のような通信キャリアの SIP インタフェースを使う場合と、VoIP TA のように、既存の PSTN 公衆網との間で、SIP のデータとアナログモデムの間で変換を行う場合もある。

特定の利用者の環境に限ってみれば、これらプロトコルのうち、すべてを使うわけではない。しかし、グローバルに製品を出荷するメーカとしては複数を搭載しておかなければならない事情がある。

過去の歴史では、こうした機能を実装した製品はそれぞれに脆弱性を持っていた。そうした脆弱性が現在の MFP には含まれていないと考えられるが、MFP の機能はソフトウェアの規模としても大きいため、必ずしもそうでない場合もあるだろう。

12.2.1 【攻撃手法とその影響】

MFPが実装する複数のプロトコルへの攻撃手法は、それぞれのプロトコルに応じて、簡単な手法から複数の手順を必要とする高度な手法まで複数の方法がある。単純な例としては、「10 ドライバ用プロトコルを経由した侵入の問題」で紹介するような、特定のプロトコルの特定命令に大きな引数を指定してバッファオーバフローさせる方法がある。また、複雑な方法の例としては「13 遠隔保守インタフェ

ースの悪用から起こる問題」で紹介するような、あらかじめブラウザで管理者ページに認証手順を済ませたあと、攻撃コードをダウンロードさせるサイトに誘導し、ブラウザに攻撃コードを実行させる、といった複雑な方法もある。

ここでは個々の詳細な手法については割愛するが、MFP の TCP/IP をベースとした主だったプロトコルについて、最近においてもさまざま脆弱性が発見されているということを紹介したい。

1) Ethernet (IEEE 802.3)の脆弱性

Ethernet (IEEE 802.3)はワイヤ上で Ethernet フレームを交換するプロトコルで、Ethernet 自体は通信データを保護する機能はない。一般的には Ethernet 用の配線や VLAN を分割して MFP の通信を分離したり、Ethernet フレームや IP パケットを暗号化するセキュリティ機能や製品を利用する。また、Ethernet はルーティング機能がなく IP よりも単純なプロトコルだが、世界レベルの広域な Ethernet 接続サービスも提供されており、予想外の範囲まで同じ Ethernet セグメントでつながっていることがあるのでネットワーク構成に注意が必要である。

最近の Ethernet 関連の脆弱性の例としては、一部の Ethernet デバイスドライバが Ethernet フレームの大きさを検査していなかった例がある(CVE-2009-4537)。また、「Broadcom NetXtreme 管理用ファームウェアにバッファオーバーフローの脆弱性(JVNVU#512705)」のように、Ethernet カード(またはモジュール)上に遠隔管理用のソフトウェアが追加されていて、脆弱性が発見される場合もある。

Ethernet は安価な標準的な通信インタフェースとして普及しながら、10 ギガビット/毎秒を超える高速通信を実現し、信頼性向上のために運用管理機能も拡充されるなど変化を続けている。

2) 無線LANの脆弱性

無線 LAN には端末と端末が直接接続を行うアドホックモードや、アクセスポイントを経由して端末が通信するインフラストラクチャモードの別があり、アドホックモードでの認証は難しい。また、他の端末の通信を中継するアクセスポイントは、本来はよく管理された状態で動作させなければならないが、目に見えない無線で接続するため第三者が偽のアクセスポイントを動作させることが簡単であり、無線 LAN 端末を偽のアクセスポイントに接続させることも容易である。

よく知られた無線 LAN の脆弱性としては、無線通信を暗号化する WEP という方式で、暗号化を行う鍵が解読されやすい問題がある。

無線LANのセキュリティについては、WPAという通信の保護方式を利用するなどの対策があり、「総務省 無線LANにおける危険性[18]」などのサイトで、安全な無線LANの使い方が紹介されている。

3) TCP/IPの脆弱性

TCP/IP の脆弱性については、IPA「TCP/IP に係る既知の脆弱性に関する調査報告書 改訂第 4 版」としてまとめられている。ARP、IPv4、ICMP、TCP、UDP についての脆弱性が含まれており、これらの脆弱性を検証するためのソフトウェア「TCP/IP に係る既知の脆弱性検証ツール V4.0 」も配布されている。

TCP/IP は一般的に OS のカーネル内で動作するため、脆弱性を攻撃されると OS

[18] 無線LANにおける危険性 - http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/ippan12.htm

が停止するなど、影響が大きい。

4)　DNSの脆弱性

DNS は www.example.jp などのホスト名を IP アドレスに変換するためのプロトコルである。ホスト名を使わず、IP アドレスだけを使う場合、DNS は不要だが、インターネットを経由したメールファクスを利用する場合は DNS が必要になることが多い。

DNS の代表的な脆弱性としては、DNS のメッセージが保護されていないことを悪用して、DNS で名前解決をしようとするホストに偽の IP アドレスを注入する「DNS キャッシュポイズニング」がある。2008 年に DKA(Dan Kaminsky Attack)という手法が発見され、影響が大きいと指摘された。その後、DNS の脆弱性に対処するため DNSSEC という保護方式が徐々に導入されつつある。

5)　SNMP、SNMPv3 の脆弱性

SNMPは主にネットワーク機器や通信機器の動作状態を監視するためのプロトコルである。SNMPでは、通信機器の内部の動作状態を示す情報にアクセスするために、MIB(Management Information Base)と呼ばれる、階層化された名前のラベルから、型つきの値を応答する処理を行う。SNMPプロトコル上では、要求と応答の両方のメッセージデータがASN.1(Abstract Syntax Notation One)というバイナリ形式で符号化されるが、ASN.1 の解釈を行う実装を中心にSNMPでは多数の脆弱性が発見されている[19]。なお、ASN.1 の実装についてはDNSでも脆弱性が発見されている。

SNMPには認証手順と暗号化手順がなかったが、SNMPv3 で追加されている、SNMPv3 については、認証手順の実装にも脆弱性が発見されている[20]。

その後、SNMP は、SNMP のメッセージの型式を定義する仕様と、SNMP メッセージの伝送を定義する仕様(RFC5590)を分離し、通信内容を保護する伝送方式を選択しやすいようにしている。

SNMP は階層化された MIB 情報をツリー上にたどりながら問合わせ処理ができる特徴がある。そのため、設定を間違えるか処理量の制限がないと、再帰的に多数の MIB 情報の問合わせが発生して機器の動作に問題が発生することがある。

また、SNMP による監視結果を元にした「アクション」などの特定の動作を定義できる実装がある。こうした実装では、偽の SNMP 応答の内容を検査しないでアクションを実行すると、任意のコマンドを実行させられることがある。

6)　FTPの脆弱性

FTP(File Transfer Protocol)は HTTP 以前からインターネットでのファイル転送の標準プロトコルであったためよく普及している。

しかし、FTP には長期にわたって通信を保護する手順がなく、制御用の TCP ポートとデータ転送用の TCP ポートが分かれている複雑な構造から、IPsec などでの通信内容の保護がしにくいといった問題があった。現在は FTP を SSL/TLS 上で利用する、制御用 TCP ポートとデータ転送用 TCP ポートを同一のポートにする、な

---

[19] SNMPでは多数の脆弱性が発見されている - IPA: 広範囲に該当する SNMP の脆弱性について - http://www.ipa.go.jp/security/ciadr/20020213snmp.html

[20] SNMPv3 の認証手順の実装にも脆弱性 - JVNVU#878044 SNMPv3 実装の不適切な HMAC 処理による認証回避の脆弱性 - http://jvn.jp/cert/JVNVU878044/

どの改良も行われているが、MFP 製品で採用しているかどうかはカタログベースでは特に記述がなく確認できなかった。

また、FTP の一部のコマンドはすでに悪用された事例がある。FTP の port コマンドは、他の FTP サーバに対して任意のホストの任意のポート番号の TCP ポートに接続させる命令である。port コマンドを悪用する例として「FTP バウンス攻撃」がある。FTP site コマンドは接続先の FTP サーバ上で任意のコマンドを実行させる機能で、この機能が残っている FTP サーバを動作させることは非常に危険である。FTP cwd コマンドは、接続先の FTP サーバ上でのカレントディレクトリを移動するコマンドである。cwd コマンドはファイルを書き込む FTP put か、ファイルを読み出す FTP get と組み合わせて利用するが、特権が必要なディレクトリやファイルへの操作がないよう、FTP サーバ上でのアクセス可能なディレクトリを一部のサブディレクトリ以下だけに限定するのが普通である。

FTP サーバの利用方法として、認証不要の anonymous FTP サーバというものがある。これは FTP プロトコルでのログイン時にユーザ名として”ftp”または”anonymous”と送信し、任意にパスワード文字列を送信すれば、誰でもその FTP サーバを利用できる使い方である。一部の FTP サーバの実装には、標準的に anonymous FTP サーバが動作するようになっていることがあり、FTP サーバの動作には注意が必要である。

以上のような状況から、MFP を利用する環境では FTP の利用には相当に充分な注意が必要だと考えられる。

最近のFTPに関する脆弱性には、Microsoft社のIISサーバのFTPサービスで、遠隔から任意のコードが実行させられる脆弱性(JVNVU#276653[21])などがある。また、「ガンブラー」と呼ばれるコンピュータウイルスの攻撃手法[22]の中には、FTPクライアントソフトのパスワード文字列を自動的に奪い、ウイルスがWebサイトを次々に改ざんし、感染コードを埋め込む攻撃手法が含まれている。

7)　HTTP、HTTPSの脆弱性

HTTP の脆弱性については、HTTP をベースにした Web サイトの脆弱性や Web ブラウザの脆弱性としてとらえることができる。HTTP プロトコル自体の脆弱性については「SE のための情報セキュリティ対策 - HTTP 脆弱性」に要点がまとめられている。Web サイトの脆弱性については「IPA: 安全なウェブサイトの作り方」に対策も含めて解説されている。

HTTP をベースとしたサービスは、Web ブラウザのグラフィカルなユーザインタフェースを活用して効率よく機能を提供できるため、非常に広範囲に利用されている。また、プリント機能を提供する「IPP(Internet Printing Protocol)」や、Web サーバ間で処理を自動化する「Web サービス」、共有ファイルへのアクセスを提供する「WebDAV」などの用途を特化したサービスも HTTP をベースにしている。このことから、HTTP の脆弱性は影響する範囲が非常に大きい。

また、HTTP の通信路を保護する HTTPS (HTTP over SSL/TLS)も非常に広く普及しているため、HTTPS の脆弱性が及ぼす影響も大きい。最近の例では SSL/TLS の renegotiation(SSL/TLS 通信中に再び接続を確立する)機能の脆弱性が報告されている。

---

[21] JVNVU#276653 - Microsoft Internet Information Services FTP サーバにおけるバッファオーバーフローの脆弱性 - http://jvn.jp/cert/JVNVU276653/

[22] 「ガンブラー」と呼ばれるコンピュータウイルスの攻撃手法 – IPA「"ガンブラー" の手口を知り、対策を行いましょう」 - http://www.ipa.go.jp/security/txt/2010/02outline.html

HTTP のプロトコル自体の脆弱性としては、基本的に HTTP の各メッセージがそれまでの状態をひきつがず、ステートレスである点がある。これは HTTP の構造が単純で使いやすいメリットの裏の側面でもある。HTTP はステートレスであるため、一連の処理が完了するまでに複数のリクエストとレスポンスを交換する場合は、アプリケーションが独自にセッション情報を維持しなければならない。

8) LDAP、Kerberosの脆弱性

LDAP と Kerberos はネットワーク上で集中的に認証・認可を行う代表的なプロトコルである。LDAP と Kerberos を効率的に利用すれば、何台もの MFP のそれぞれに利用者登録をすることなく認証ができて、パスワードの更新も集中管理できる。しかし、認証情報や権限認可情報が集中している分、影響も大きい。

LDAP 自体には通信内容を保護する機能がないため、SSL/TLS と組み合わせて利用する。Kerberos はバージョン 4 以降で、暗号化する機能がプロトコルに組み込まれている。また、LDAP サーバに対しては、ID やメールアドレスなどの検索を要求するときに、SQL インジェクションを実行させる引数が含められることがある。

最近のLDAPの脆弱性には「JVNDB-2009-001779 - Active Directory の LDAP サービスにおけるサービス運用妨害(DoS) の脆弱性[23]」などがある。Kerberosについては「JVNDB-2010-001344 - MIT Kerberos の kadmind におけるサービス運用妨害 (DoS) の脆弱性[24]」などがある。

9) SMBの脆弱性

SMB(Server Message Block)はファイル共有サービスを提供するプロトコルである。CIFS という、SMB の上位バージョンのプロトコルも提供されているが、一般的には CIFS も含めて SMB と呼ばれている。

SMB のファイル共有サービスでは、MFP からスキャンしたファイルを転送したり、MFP 内部に格納されたスキャンイメージを利用者端末から取り出したりする形で利用する。また、ファクス受信で到着したファクスイメージを MFP から利用者端末に対して直接転送することもある。さらに MFP にプリントを要求するときに利用することも可能である。

SMBでは、NTLMと呼ばれる認証手順が利用されてきたが、NTLMではパスワードを交換するとき、生のパスワードを解読しやすい問題があり、NTLMv2 という改良された手順がある。SMBで利用されるNetBIOSというプロトコルでは、ブロードキャストを利用してSMBサーバの名前をIPアドレスに解決するため任意の偽の応答にだまされやすい。また、Windows XP SP1 以前のWindowsで動作するSMBファイル共有サーバでは、ファイル共有機能がパスワードなしでも動作する脆弱性[25]があった。

SMBはWindows端末の標準機能であり、よく普及しているため脆弱性も多数発見されていてウイルスやマルウェアの形となった攻撃コードも多い。最近のSMBの脆弱性には「JVNVU#135940 - Windows SMB version 2 に脆弱性[26] (遠隔の第三者に

---

[23] JVNDB-2009-001779 - Active Directory の LDAP サービスにおけるサービス運用妨害 (DoS) の脆弱性 - http://jvndb.jvn.jp/ja/contents/2009/JVNDB-2009-001779.html

[24] JVNDB-2010-001344 - MIT Kerberos の kadmind におけるサービス運用妨害 (DoS) の脆弱性 - http://jvndb.jvn.jp/ja/contents/2010/JVNDB-2010-001344.html

[25] ファイル共有機能がパスワードなしでも動作する脆弱性
http://itpro.nikkeibp.co.jp/members/NBY/techsquare/20021129/3/

[26] JVNVU#135940 - Windows SMB version 2 に脆弱性 - http://jvn.jp/cert/JVNVU135940/

よって、任意のコードが実行させられたり、サービス運用妨害 (DoS) 攻撃を受けたりする)」などがある。

10) SIPの脆弱性

SIP(Session Initiation Protocol)は既存の PSTN 公衆網、いわゆる電話の伝送を IP で行うためのプロトコルである。MFP では、ファクスの伝送のために、SIP と RTP(Real-time Transport Protocol)を利用する。

SIP は通信内容を保護するためのいくつかの仕様があるが、通信事業者の間では、通信事業者内だけで SIP の通信をする前提となっているため、一般的に通信の保護機能は利用されていない。一方で、SIP を利用した製品などの実装では、通信の保護機能がなくても、IP アドレスを指定すればインターネット上の SIP サーバや SIP 端末とも通信できてしまう脆弱性がある。また、SIP については電子メールの迷惑メールのような「SPIM」と呼ばれる「迷惑着信」の問題もある。

SIPの脆弱性についてはIPA「SIPに係る既知の脆弱性に関する調査報告書 改訂第 2 版」[27]に詳述されている。また、この脆弱性に対応するIPA「SIPに係る既知の脆弱性検証ツール V1.0」[28]も配布されている。

11) SMTP、POP3、IMAP4 の脆弱性

SMTP は電子メールの転送を、POP3 と IMAP4 はメールボックスへのアクセスを提供するプロトコルである。これらも HTTP 以前から存在し、普及している。

SMTP については、もともと認証手順も通信の保護手順も仕様になかったため、さまざまな問題が発生していた。現在も、商品の広告やコンピュータウイルスを添付した「迷惑メール」が大量に届いてしまう問題などがある。

また、これらの電子メールのプロトコルの実装にもさまざまな脆弱性が発見されてきた。SMTP のコマンドについては、認証なしでメールアドレスの存在確認ができる SMTP vrfy コマンドと、別名アドレスやメーリングリストのメンバー名を展開できる SMTP expn コマンドの脆弱性がある。SMTP auth コマンドは SMTP プロトコルで SMTP クライアントの認証を行う手順だが、パスワード文字列をハッシュ化して交換するため SMTP auth 手順を盗聴されるとパスワードを解読される可能性が高い。さらに SMTP 自体にはメッセージや SMTP の通信路を保護する機能がないため、SMTP を安全に利用するには SSL/TLS か IPsec で SMTP 通信路を保護する必要がある。

最近のSMTPの脆弱性には「Microsoft Windows の SMTP コンポーネントにおける情報漏えいの脆弱性[29]」などがある。POP3 については認証用のパスワード交換手順の脆弱性として「APOPにおけるパスワード漏えいの脆弱性[30]」などがある。最近の事例ではPOP3 とIMAP4 の両方で、応答処理の脆弱性として「複数の Microsoft 製品の inetcomm.dll における整数オーバーフローの脆弱性[31]」が報告さ

---

27 IPA「SIPに係る既知の脆弱性に関する調査報告書 改訂第 2 版」- http://www.ipa.go.jp/security/vuln/vuln_SIP.html

28 IPA「SIPに係る既知の脆弱性検証ツール V1.0」- http://www.ipa.go.jp/security/vuln/vuln_SIP_Check.html

29 JVNDB-2010-001391 - Microsoft Windows の SMTP コンポーネントにおける情報漏えいの脆弱性 - http://jvndb.jvn.jp/ja/contents/2010/JVNDB-2010-001391.html

30 JVNDB-2007-000295 - APOP におけるパスワード漏えいの脆弱性 http://jvndb.jvn.jp/ja/contents/2007/JVNDB-2007-000295.html

31 JVNDB-2010-001471 - 複数の Microsoft 製品の inetcomm.dll における整数オーバーフロ

れている。
S/MIMEは電子メールのメッセージを安全に交換するための、メッセージやコンテンツの保護仕様である。S/MIMEの保護を確実にするには電子証明書を正しく運用する必要がある。また、S/MIMEではメールの宛先や送信元などを示すメールヘッダは保護されない、などの注意事項をよく理解する必要もある。詳しいS/MIMEの利用方法はIPA「電子メールのセキュリティ - S/MIME を利用した暗号化と電子署名[32]」を参照いただきたい。

12.2.2 【原因と考察】

1) プロトコルの多さ

MFPには、認証のないDNSやDHCPなどのような歴史的なプロトコルから、IPPやWebサービスのような複雑な認証手順を標準化したプロトコルまでさまざまなレベルのプロトコルが混在している。MFPの業界団体であるJBMIAが配布しているBMLinkS[33]のように、複数メーカの複数機種のMFPに対応する共通ドライバを開発する活動もあるが、既存のプロトコルは利用者端末の条件や他システムとの制約などの依存関係を相互に持っており、簡単にいずれかひとつのプロトコルには集約できない、という状況がある。

2) 今なお発見される脆弱性には、事後対応も含めた対策

MFP は本体の機能も豊富な上、ネットワーク上で MFP 本体と協調動作するユーティリティや特定の変換や処理を行うソフトも含めると、MFP に関連するソフトウェアは数十本以上にのぼり、ソフトウェアの規模が非常に大きい。
そのため、MFPの脆弱性はどうしてもゼロにはできないという状況もある。一説には、ソフトウェアについての脆弱性は、よく管理された開発現場でもソースコード 1 千行から 1 万行あたり 1 件は存在するとも言われる[34]。「12.2.1【攻撃手法とその影響】」で列挙したように、どのプロトコルにもどこかの実装で脆弱性が報告されている。
MFP の脆弱性は完全にゼロにはできないとすれば、MFP の利用者も、MFP を製品として提供す側も、それぞれが脆弱性に事後対応することを想定しておく必要があるだろう。脆弱性への利用者としての事後対応については、利用している製品に関する脆弱性情報と対応策についてメーカから情報収集することや、そのあとソフトウェアの更新や利用手順の変更などの対応を想定した体制を整えておく、もし被害が起こったときのための担当者と対応手順を検討しておく、などがある。
製品を提供する側での脆弱性への事後対応の例としては、脆弱性の確認と報告の手順、被害と脅威の低減方法の検討、製品への反映方法の検討、対応の優先度づけ、などがあるだろう。

一の脆弱性 - http://jvndb.jvn.jp/ja/contents/2010/JVNDB-2010-001471.html
[32] IPA「電子メールのセキュリティ - S/MIME を利用した暗号化と電子署名」 http://www.ipa.go.jp/security/fy12/contents/smime/email_sec.html
[33] BMLinkS – JBMIA: 社団法人ビジネス機械・情報システム産業協会 BMLinkSプロジェクト委員会http://www.jbmia.or.jp/bmlinks/
[34] 脆弱性はソースコード千行から 1 万行に 1 件 - 「セキュリティの神話」JohnViega著、葛野弘樹　監訳、夏目 大　訳、2010 年 4 月、オライリー・ジャパン

3)　複数のプロトコル実装に含む脆弱性への対策

こうした多数のプロトコルを同時に実装せざるを得ない状況で、MFP製品の脆弱性を最小限に抑えるための設計、開発者向けの対策として、IPAで普及活動を行っている「セキュリティエンジニアリング」[35]や「セキュア・プログラミング講座」[36]、「組込みシステムのセキュリティへの取組みガイド」[37]などがある。

これら脆弱性対策の取り組みでは、既存の方法では検討事項や試験項目が増えすぎて対応が難しい。そのため、いくつかの自動化された試験ツールや検査方法の利用も検討が必要だろう。

試験ツールには、ソースコードを検査して脆弱性を発見するツール[38]や、製品のHTTP通信などの機能をブラックボックス的に外部から試験して脆弱性を発見する製品がある。脆弱性の検査を行うことでよく知られている製品としてはCodenomicon[39]、AppScan[40]、Nessus[41]などがあり、MFP製品の脆弱性検査にも有用だと考えられる。また、こうした脆弱性試験手順を含む評価手順についてはMicrosoftのWindows Logo[42]で行われているような、脆弱性のテストを含む製品認証制度も参考になるだろう。

---

35 IPA「セキュリティエンジニアリング」- http://www.ipa.go.jp/security/awareness/vendor/software.html
36 IPA「セキュア・プログラミング講座」- http://www.ipa.go.jp/security/awareness/vendor/programming/
37 IPA「組込みシステムのセキュリティへの取組みガイド」- http://www.ipa.go.jp/security/fy20/reports/emb_app/
38 IPA「セキュア・プログラミング講座C/C++言語編」ソースコードレビュー http://www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/c103.html
39 Codenomicon - http://www.codenomicon.com/
40 AppScan - http://www-06.ibm.com/software/jp/rational/products/test/appscan/
41 Nessus - http://www.nessus.org/nessus/
42 Windows Logo - http://www.microsoft.com/japan/whdc/winlogo/hwrequirements.mspx Windows 用デバイスドライバ向けに提供されている製品認証試験制度

12.3 対策

12.3.1 【運用ガイド】

1) MFP 上で利用する機能を必要最小限に特定し、利用しない機能をすべて停止する
2) メーカの脆弱性対策情報を購読するか、いつでも入手できるように準備する
3) 監査記録から、利用動向、セキュリティ違反の動向を定期的に把握し、対策する
4) MFP 製品の脆弱性が発見された場合の対応方法を計画しておく
5) 脆弱性の被害が発生したときの対応方法を計画しておく

12.3.2 【実装ガイド】

1) 製品の企画、開発のプロセスを通じて、製品の脆弱性対策に取り組む
2) MFP を利用する環境で適用されるセキュリティポリシを MFP にも容易に強制しやすくなるようなツールを検討する
3) 脆弱性検査ツールとして、ソースコードの静的分析ツール、ファジングツール、侵入テストツールなどの利用を検討する
4) 脆弱性が発見された場合の対応を行う体制を整え、対応手順を計画しておく

12.4 参考情報

公開年月	情報源
2001 年	IPA - 電子メールのセキュリティ - S/MIME を利用した暗号化と電子署名 http://www.ipa.go.jp/security/fy12/contents/smime/email_sec.html S/MIME の正しい利用方法など
2002 年 2 月	IPA: 広範囲に該当する SNMP の脆弱性について http://www.ipa.go.jp/security/ciadr/20020213snmp.html SNMPv1 の脆弱性に関する情報
2008 年	SE のための情報セキュリティ対策 - HTTP 脆弱性 http://www.chuu-information.com/security/fragile_6.html HTTP プロトコル自体の脆弱性の要点がまとめられている
2008 年 6 月	JVNVU#878044 SNMPv3 実装の不適切な HMAC 処理による認証回避の脆弱性 http://jvn.jp/cert/JVNVU878044/ SNMPv3 で特定のメッセージにより認証が回避されてしまう脆弱性
2008 年 7 月	DNS Cache Poisoning の概要と対処 http://www.nttv6.net/files/DKA-20080723.pdf 攻撃持続時間と攻撃の成功率を示すグラフ、DKA 手法解説など
2009 年 1 月	IPA: TCP/IP に係る既知の脆弱性に関する調査報告書 改訂第 4 版 http://www.ipa.go.jp/security/vuln/vuln_TCPIP.html TCP, ICMP, IPv4, ARP プロトコルの解説つき脆弱性資料。
2009 年 1 月	IPA: TCP/IP に係る既知の脆弱性検証ツール V4.0 http://www.ipa.go.jp/security/vuln/vuln_TCPIP_Check.html TCP, ICMP, IPv4, ARP と、一部 IPv6 に対応

2009 年 4 月	IPA - SIP に係る既知の脆弱性に関する調査報告書 改訂第 2 版 http://www.ipa.go.jp/security/vuln/vuln_SIP.html SIP, SDP, RTP, RTCP の脆弱性、実装上の脆弱性、SIP/RTP の暗号化など
2009 年 4 月	IPA - SIP に係る既知の脆弱性検証ツール V1.0 http://www.ipa.go.jp/security/vuln/vuln_SIP_Check.html 脆弱性の再発防止のため、SIP 実装製品の開発者向けに無償貸出
2009 年 7 月	IPA: 組込みシステムのセキュリティへの取組みガイド http://www.ipa.go.jp/security/fy20/reports/emb_app/ 組込みシステムのライフサイクルを通じたセキュリティ対策手順
2009 年 11 月	JVNVU#120541 SSL および TLS プロトコルに脆弱性 http://jvn.jp/cert/JVNVU120541/ SSL/TLS の通信中に再び接続を確立する機能の脆弱性
2009 年 12 月	CVE-2009-4537: r8169: straighten out overlength frame detection http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4537 Realtek 製 Ethernet チップのドライバに含まれていたフレーム長検査の不良
2010年 2 月	IPA「"ガンブラー" の手口を知り、対策を行いましょう」 http://www.ipa.go.jp/security/txt/2010/02outline.html 正規 WEB サイトの改ざん、FTP クライアントソフトの ID とパスワードの奪取、など
2010 年 3 月	IPA - 安全なウェブサイトの作り方 改定第 4 版 http://www.ipa.go.jp/security/vuln/websecurity.html 対策チェックリスト、安全な SQL の呼び出し方などもある
2010 年 5 月	IPA - セキュア・プログラミング講座 http://www.ipa.go.jp/security/awareness/vendor/programming/ 開発、品質保証部門向けの脆弱性解説とチェックリスト
2010 年 5 月	IPA - セキュリティエンジニアリング http://www.ipa.go.jp/security/awareness/vendor/software.html 設計、開発部門向けのセキュリティ開発ガイド

12.5 CVSS深刻度評価(参考値)

解説では複数のプロトコルについて紹介したが、ここではそのうちの一例だけについて、被害の影響を CVSS 2.0 で評価する。評価する例は、MFP 内部の HTTP サーバが、攻撃用に整えられた GUI つきツールを使った攻撃で侵入され、任意のコードが実行させられることはないが、動作が不安定になりサービスが停止した場合を想定する。

12.5.1 【評価結果】

本脆弱性の深刻度	□Ⅰ（注意）	■Ⅱ（警告）	□Ⅲ（危険）
本脆弱性の CVSS 基本値		5.8	
本脆弱性の CVSS 現状値		5.0	

12.5.2 【CVSS基本値の評価内容】

攻撃元区分	□ローカル	■隣接	□ネットワーク
攻撃条件の複雑さ	□高	□中	■低
攻撃前の認証要否	□複数	□単一	■不要
機密性への影響	□なし	■部分的	□全面的
完全性への影響	□なし	■部分的	□全面的
可用性への影響	□なし	■部分的	□全面的

12.5.3 【CVSS現状値の評価内容】

攻撃される可能性	□未実証	□実証可能	□攻撃可能	■容易に攻撃	□未評価
利用可能な対策のレベル	■正式	□暫定	□非公式	□なし	□未評価
脆弱性情報の信頼性	□未確認	□未確証	■確認済み		□未評価

13. 遠隔保守インタフェースの悪用から起こる問題

13.1 概要

攻撃者が MFP の遠隔保守インタフェースを悪用することにより、MFP 内部の情報と MFP に関連する他システムの情報が攻撃者に不正に入手される。

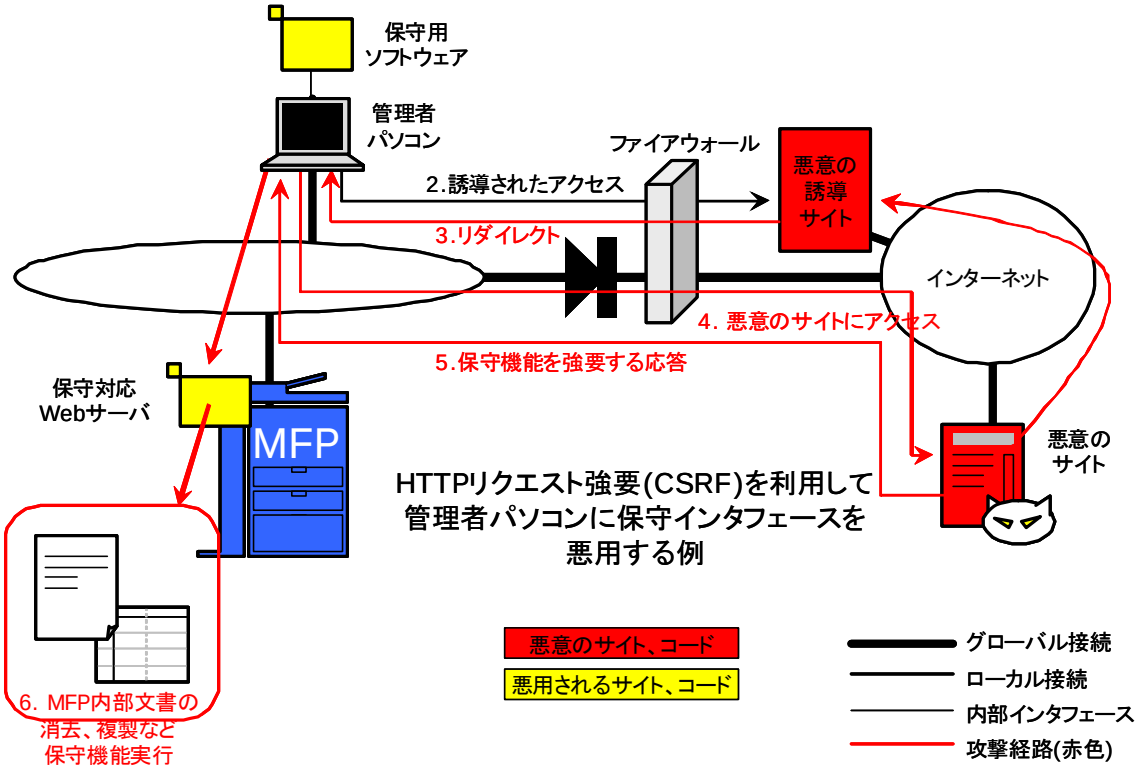

図 13-1 HTTP リクエスト強要(CSRF)を利用した MFP の保守インタフェース悪用例

13.2 解説

13.2.1 【攻撃手法とその影響】

MFP の保守機能は、一般的にはコピー枚数やトナーの残量、故障診断と故障部品の交換修理がある。このうち、故障したハードディスクを交換するために、以下のような機能がある。

1) MFP内部の文書ファイル、アドレス帳を一括してバックアップする機能
2) MFP内部の文書ファイル、アドレス帳を一括して所定のファイルから上書きする機能
3) MFP内部の文書とアドレス帳を一括して削除、上書き消去する機能

1)文書ファイルをバックアップする機能では、MFP 内部のハードディスクに格納されている文書を一括して MFP の外部に取り出すことができる。この機能は MFP 内部の HDD が故障したときに、新しい HDD と交換するために必要な機能で

ある。

2)の MFP 内部の文書ファイルなどを所定のファイルから上書きする機能は、1)で保存しておいた HDD のバックアップデータを使って HDD の内容を復元する機能である。「レストア(restore)」または「リストア」とも呼ばれる。

3)の MFP 内部の文書とアドレス帳を一括して削除、上書き消去する機能は、交換対象の廃棄が必要なハードディスクの内容を消去するために利用される。また、MFP を廃棄するときに MFP 内部の情報が第三者に漏洩しないようにするためにも利用される。

MFP内部の保守用インタフェースは、本体のコンソールパネルからのメニュー操作のほか、下の図 13-2のような保守専用のインタフェースも一部の機種で存在すると考えられる。

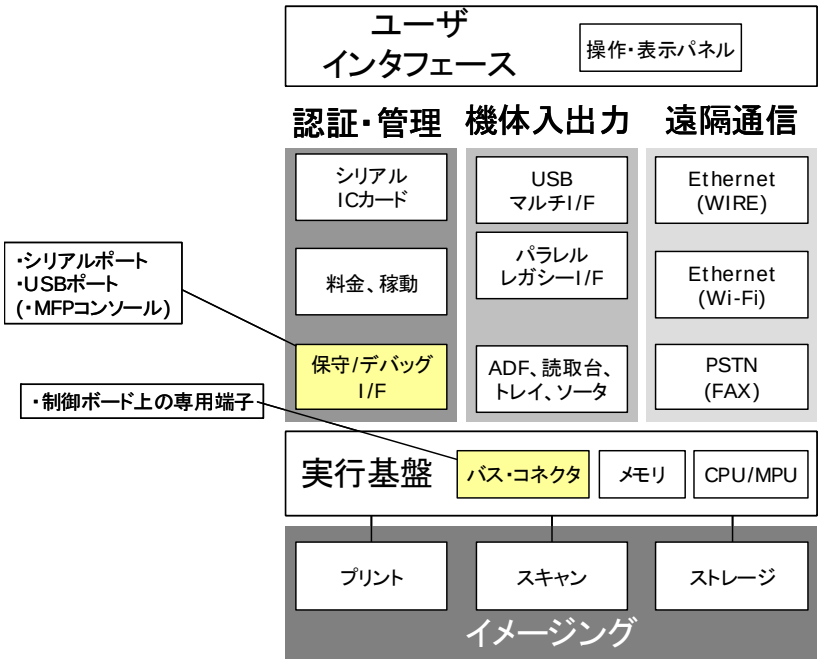

図 13-2 MFP 機器内部の保守インタフェース

しかし、上記のような MFP 内部のインタフェースでは、MFP の保守作業を行うために MFP が設置された場所に出向かなければならないため、ネットワークを経由して遠隔から保守を行うための機能が提供されている。ここではこれら機能を遠隔保守機能と呼ぶことにする。

下の図 13-3の左上の一般利用者端末と管理者端末のように、遠隔保守機能は一般的には組織内のネットワーク上の端末から実行する。また、メーカや保守業者が提供する遠隔保守サービスを利用している場合は、図 13-3の右上にあるような組織外のネットワークを通じて遠隔保守のための通信を行っている。また、MFP本体に直接接続する保守インタフェースを使う場合も一部であるだろう。

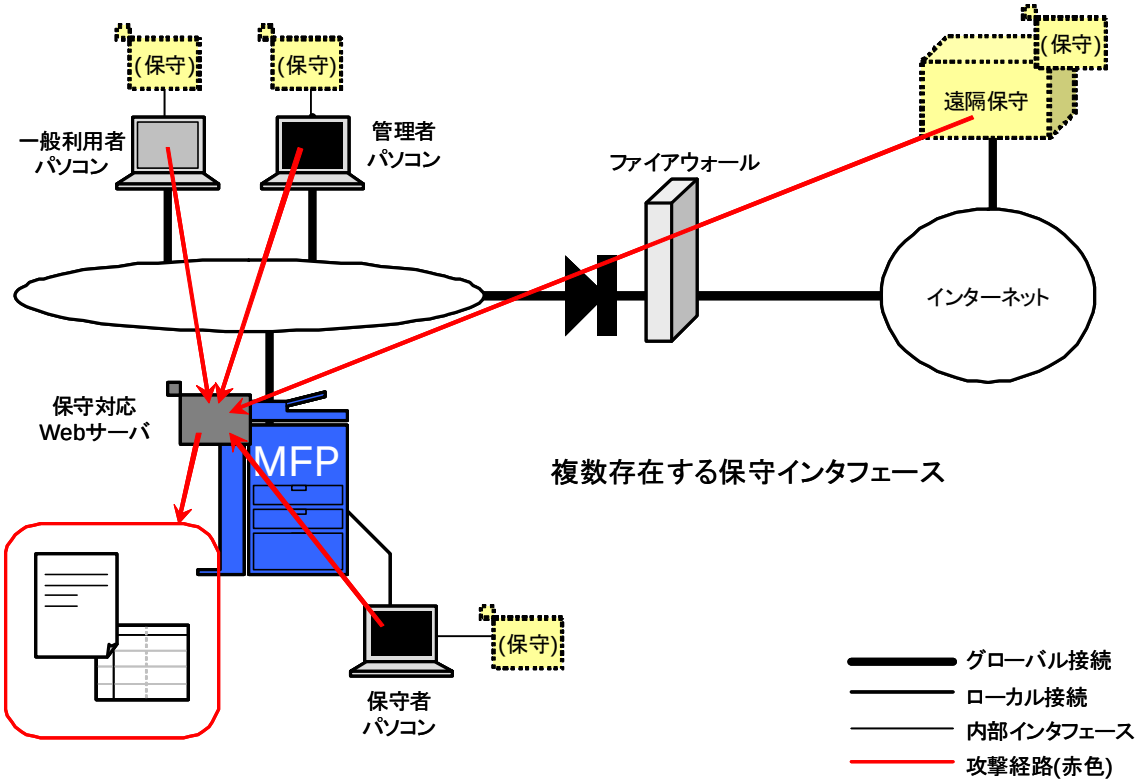

図 13-3 その他の MFP の保守インタフェースへのアクセス方法例

このように遠隔保守機能には複数の経路がある。このうち、ここではある管理者が利用者のネットワーク内部で MFP の遠隔保守用機能を Web ブラウザからネットワーク経由で利用する場面を想定する。
下の図 13-4は、遠隔保守機能を利用する管理者のWebブラウザにCSRFリクエスト強要攻撃を行い、攻撃者から見て認証なしで、管理者のWebブラウザにMFP内のデータを消去させる操作を行う例である。
管理者はいったん MFP の認証ページで管理者認証を行い、保守機能のページを開く。ブラウザが保守機能のページを開いたままの状態で、赤線で示すような特定の URL を開かせる JavaScript コードを管理者のブラウザに注入することで、認証手順なしで、MFP の内部データ消去などの保守機能を実行させられる。

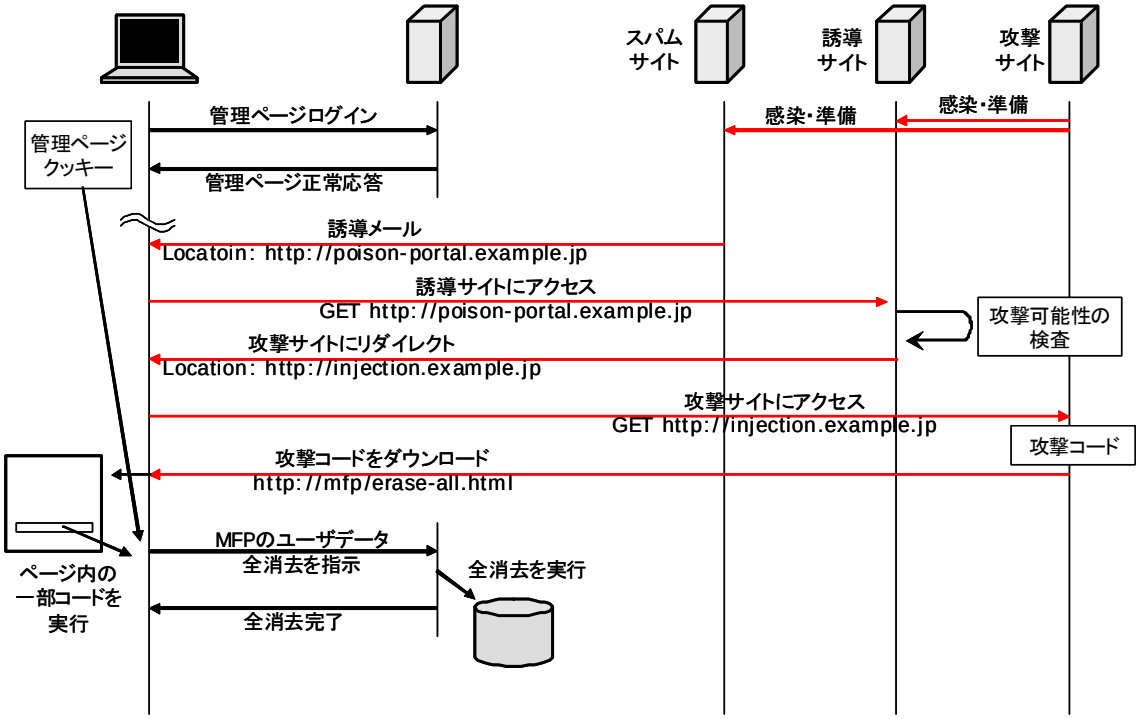

図 13-4 CSRF を利用した保守インタフェース悪用のシーケンス例

この攻撃手法にはいくつかの条件がある。MFP の型番が特定でき、管理者が保守機能を利用するためのページであらかじめ開いたままにしておくか、ログイン認証を成功させてブラウザ上に HTTP クッキーなどの形で認証情報を保存しておかなければならない。また、管理者端末のブラウザを特定サイトに誘導し、攻撃コードをダウンロードさせる必要である。さらに、保守機能を提供する MFP の管理ページに、CSRF 脆弱性が含まれている必要がある。

そのため一般的にはこの攻撃手法が現実に成功することは少ないと考えられるが、利用者のサイト内や、ビデオで撮影されている環境などのように、管理者の動作や作業がよく見て取れるような状況では、攻撃のチャンスが高まるだろう。

なお、遠隔地から保守作業を行う遠隔保守サービスでは、MFP 自体が遠隔保守サイトにアクセスし、簡易的に VPN のような専用接続を設定する方法などがあり、IP アドレス変換やファイアウォールを設定した利用者のネットワークにおいても容易に利用可能である。

13.2.2 【原因と考察】

MFP 機器本体の保守インタフェースは MFP 機器本体内部の一部の故障部品を交換するときなどのため、内部情報をバックアップするなどの重要機能を持っている。一般的には MFP メーカの保守担当者や委託業者が保守作業を行うが、利用者の利便性のため、一部の保守機能が利用者側に開示されている場合がある。また、専用の保守用ソフトウェアが一部利用者に開示されている場合もある。

こうした保守機能は便利な反面、HDD の交換や MFP を廃棄するための機能については、MFP の取扱説明書で明確に記述されていない場合もある。部品の交換は MFP の保守業者の役目だが、文書情報などを含む HDD の内容については利用者に管理責任があるため、HDD の交換を行う際は利用者か管理者が HDD の内容をバックアップする必要がある。ただし本調査では、HDD の内容の取り扱いについて

は保守業者が交換時にバックアップとリストアをすることもありえると仮定した。利用者としてはHDDの交換作業やバックアップとリストアの方法や注意について一般的には知識がない場合も多く、保守業者に依頼するメリットが大きい。

また、MFP は機能増加とともに運用性も期待されており、このような保守機能の開放はユーザにとってメリットがある。

このように MFP の利便性が高まると、同時に脅威も増大する。特に保守インタフェースが MFP 本体内部の専用インタフェースだけではなく、ネットワーク上のパソコンや遠隔サイトに開放されることで、侵入される可能性が高まる。また、HDD の内容を保守業者のような第三者が扱うことに対して、どのような保護や対策がとれるかも問題になる。

現在のところ、MFP のバックアップ機能を提供するユーティリティを提供している MFP メーカはすべてではないが、MFP の利用者へのサービス停止時間を短くし、高度な MFP の機能をいつでも継続的に利用するために、バックアップ機能を活用するための対策がいくつか考えられる。主な対策としては、バックアップと消去などの重要な保守機能は利用できる範囲を特定する、バックアップデータそのものが暗号化などで保護されること、などがあるだろう。

13.3 対策

13.3.1 【運用ガイド】

1) 保守機能の何を誰がどこから利用するか、MFP を利用する前に具体的に定義し、不要な場所・組織から保守機能を利用しない
2) 保守業者が提供する遠隔保守サービスとの接続時の相互認証方式と保護法式を特定し、正しく運用する
3) 利用者がネットワーク上で保守機能を利用する際は通信路を保護するか、別ネットワークに隔離して利用する
4) ネットワーク構成やアドレス構成が変わったときのため、保守機能の稼動履歴の記録と不正利用の監視・記録を行い、定期的に監査する

13.3.2 【実装ガイド】

1) 保守機能をネットワーク上で公開することの危険性の周知
2) 保守機能設定機能での警告表示と、他のインターネット設定などとの矛盾の検査
3) 遠隔保守機能でのセキュリティ設定のデフォルト化
4) バックアップしたデータが暗号化などで保護される機能を提供する

13.4 参考情報

公開年月	情報源
2009 年 6 月	CWE-352 クロスサイトリクエストフォージェリ（リクエスト強要攻撃） http://jvndb.jvn.jp/ja/cwe/CWE-352.html

13.5 CVSS深刻度評価(参考値)

遠隔保守機能のうち MFP 内部の全データを削除する機能が CSRF リクエスト強要攻撃で強制されたときの影響を CVSS 2.0 で評価した。

13.5.1 【評価結果】

本脆弱性の深刻度	□Ⅰ（注意）	■Ⅱ（警告）	□Ⅲ（危険）
本脆弱性の CVSS 基本値		6.6	
本脆弱性の CVSS 現状値		5.3	

13.5.2 【CVSS基本値の評価内容】

攻撃元区分	□ローカル	□ 隣接	■ネットワーク
攻撃条件の複雑さ	■高	□中	□低
攻撃前の認証要否	□複数	□単一	■不要
機密性への影響	□なし	□部分的	■全面的
完全性への影響	□なし	■部分的	□全面的
可用性への影響	□なし	■部分的	□全面的

13.5.3 【CVSS現状値の評価内容】

攻撃される可能性	■未実証	□実証可能	□攻撃可能	□容易に攻撃	□未評価
利用可能な対策のレベル	□正式	□暫定	■非公式	□なし	□未評価
脆弱性情報の信頼性	□未確認	□未確証	■確認済み		□未評価

14. 着脱式媒体を利用した MFP の構成変更による問題

14.1 概要

MFP 本体の実行基盤に搭載された SD カードスロットは、所定のファイルを含む SD メモリカードを挿入して所定の操作をすることで、MFP の設定と構成を一括して更新する機能を持つようになってきた。

この機能が悪用されると、MFP を構成する証明書やパスワード、アドレスが攻撃者に漏洩したり、攻撃者によって MFP 内部の構成や設定を変更されたり、任意の MFP 用のソフトウェアが追加されたりする場合がある。

なお、着脱式媒体を利用した MFP の一括更新機能については、一般的には公開されている情報はなく、MFP 有識者にヒアリングした情報をもとに作成している。

14.2 解説

14.2.1 【攻撃手法とその影響】

2008 年ごろから、MFP では本体の実行基盤に SD カードスロットを装備し、簡単に MFP のソフトウェア的な構成を一括変更できる機能が搭載されるようになった。この背景としては MFP が設置されるネットワーク環境は認証 VLAN などで厳しく接続が制限されている場合が多く、簡単に管理者端末や保守者端末を接続できない事情がある。また、出荷後の MFP を納品先で一括して設定変更できると、出荷時のコストを抑えることができ、顧客の要望にも対応しやすく、設置時の作業時間も削減でき、MFP の製造・販売者と利用者の両方にメリットがある。

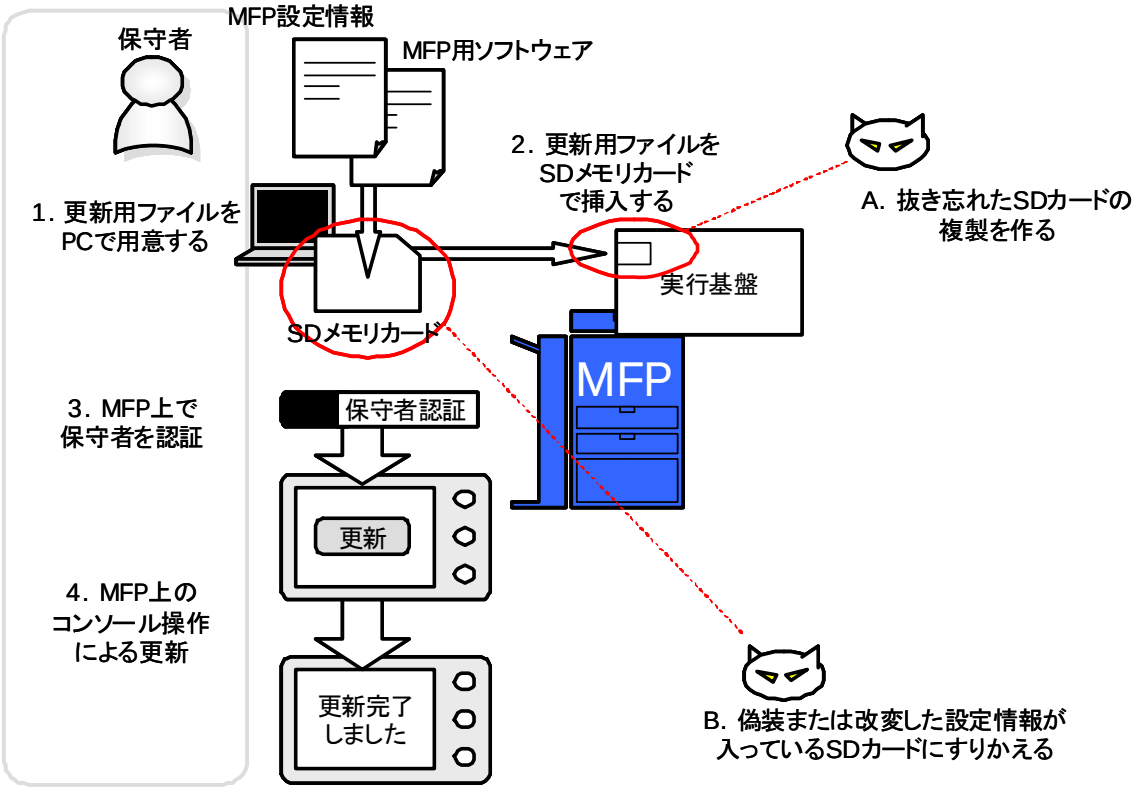

図 14-1 SD メモリカードによる MFP の一括更新による問題

上の図 14-1の左半分では、SDメモリカードによるMFP内部の設定とソフトウェアの一括更新の手順の概要を示している。まず、保守者はあらかじめ所定の設定とソフトウェアのファイル群を同梱したSDメモリカードを作成しておく。SDメモリカード内でのファイルの形式や名前、配置方法は各MFPメーカの形式があるもようだが、一般公開されている取扱説明書には記載がないため、詳細は不明である。

保守者は準備された SD メモリカードを MFP 本体の実行基盤ユニットの SD カードスロットに挿入し、MFP 本体のコンソールから保守者認証などの特権の認証を行ったあと、所定の操作で MFP の設定・ソフトウェアの一括更新を MFP に指示すると、MFP 内部で SD メモリカード内のファイルの内容に従って処理が実行され、更新が完了する。

この機能を悪用して、A.攻撃者は抜き忘れられた SD メモリカードのコピーを作成して、B.偽装した更新情報、改変した設定情報が入っている SD カードをすりかえて更新に利用させる、などの攻撃が想定できる。また、攻撃者が保守者の ID とパスワードを盗み出し、保守者になりすまして保守者認証を行い、SD メモリカードを使って一括更新することも想定できる。

この攻撃による影響として、設定情報の中にある証明書やパスワードが攻撃者に漏洩する問題がある。MFP に設定する証明書やパスワードは、MFP 本体のもの以外にも他のメールサーバや共有ファイルサーバ、SIP ゲートウェイや、業務システムなどの他システムのものも含まれるだろう。一括設定用の設定ファイルの中には、こうした情報が含まれる可能性がある。

また、MFP 用のソフトウェアについては、ライセンス情報とともに投入されるため、必ずしも偽造が可能ではないが、ライセンス情報がソフトウェアとともに漏洩することで、そのソフトウェアのライセンス契約のないサイトでソフトウェ

アが不正に利用されることも考えられる。
　また、さらに攻撃者がソフトウェアとその追加方法を割り出すことができると、MFP 内部のジョブデータや制御状態を監視するソフトウェアなどを注入することができるようになり、継続的に MFP 内部の情報が盗聴、改ざんされるか、ソフトウェアの交換もできなくなるほどの機能停止など、全面的な被害を受ける可能性がある。
　なお、この攻撃手法については、機能と手順そのものが広く公開されていないため、一般的には実現が難しい手法である。

14.2.2 【原因と考察】

　この攻撃手法は一般的に公開されている取扱説明書には記載が見当たらないため、実現が難しい手法である。しかし、非公開の取扱説明書でも、一部の資料が海外の Web サイトで不正に販売されていることもあり、かならずしも「公開していないので安全」とは言えない面がある。
　また、MFP の管理者を含めた利用者の環境では、基本的に取扱説明書に記載された用途と機能について、情報セキュリティ上の対策をとることしかできない。そのため、取扱説明書に記載がない機能は安全というよりはむしろ隠れた脆弱性になる可能性が高い。

14.3 対策

14.3.1 【運用ガイド】

1) 保守者認証用のパスワードを適切に登録して運用する
2) 有効にしている保守機能については、メーカから取扱説明書を入手し、セキュリティ対策を検討する
3) 自動一括更新機能について、保守作業が終了したあとは無効にする
4) 通常の運用中は自動一括更新機能が無効になっていることを確認する
5) MFP の実行基盤ユニットにある SD カードスロットには何も挿入されていないことを確認する

14.3.2 【実装ガイド】

1) 利用者または管理者が自動一括更新機能の無効を確認できる機能を提供する
2) 実行基盤ユニットの SD カードスロットの動作を無効にする機能を提供する

14.4 参考情報

公開年月	情報源
(2010 年 5 月)	(MFP 有識者にヒアリングした情報をもとに作成)

14.5 CVSS深刻度評価(参考値)

MFP 本体の実行基盤上にある SD カードスロットで自動一括実行が悪用され、不正なソフトウェアが注入され継続的に MFP が扱う機密の文書が漏洩する場合の深刻度を CVSS 2.0 で評価した。

14.5.1 【評価結果】

本脆弱性の深刻度	□ Ⅰ（注意）	■ Ⅱ（警告）	□Ⅲ（危険）
本脆弱性の CVSS 基本値		6.6	
本脆弱性の CVSS 現状値		4.4	

14.5.2 【CVSS基本値の評価内容】

攻撃元区分	■ローカル	□ 隣接	□ネットワーク
攻撃条件の複雑さ	□高	■中	□低
攻撃前の認証要否	□複数	■単一	□不要
機密性への影響	□なし	□部分的	■全面的
完全性への影響	□なし	□部分的	■全面的
可用性への影響	□なし	□部分的	■全面的

14.5.3 【CVSS現状値の評価内容】

攻撃される可能性	■未実証	□実証可能	□攻撃可能	□容易に攻撃	□未評価
利用可能な対策のレベル	■正式	□暫定	□非公式	□なし	□未評価
脆弱性情報の信頼性	■未確認	□未確証	□確認済み		□未評価

15. まとめ

本調査で、MFP は、ハードウェア・ソフトウェアとも多機能な分、構成が複雑かつ搭載するプロトコルも多彩な組込み機器なので、本体インタフェースへの攻撃とネットワーク経由の攻撃による様々な脅威にさらされていることが明確になった。

MFP は日本を代表するセキュリティ製品として成長してきたが、そのセキュリティレベルの高さと信頼性を維持するため、今後、将来想定されるインターネットやクラウドサービスなどとの連携機能を視野にした調査も近い将来求められると考えられる。